PATENT
450100-04708

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

TITLE: ENCRYPTION LEVEL INDICATOR CALCULATION METHOD AND COMPUTER PROGRAM

INVENTOR: Shoji KANAMARU

William S. Frommer
Registration No. 25,506
FROMMER LAWRENCE & HAUG LLP
745 Fifth Avenue
New York, New York 10151
Tel. (212) 588-0800

S03P0958

ENCRYPTION LEVEL INDICATOR CALCULATION METHOD AND COMPUTER PROGRAM

BACKGROUND OF THE INVENTION

The present invention relates to an encryption level indicator calculation method and a computer program. To put it in more detail, the present invention relates to an encryption level indicator calculation method for calculating an indicator for evaluating safety and level of a common-key block encryption method as well as relates to a computer program implementing the encryption level indicator calculation method.

There is a variety of encryption processing algorithms, which can be roughly classified a public key encryption method and a common-key encryption method. The public key encryption method is an encryption method, which sets an encryption key and a decryption key as different keys such as a public key and a private key. On the other hand, the common-key encryption method is an encryption method, which sets an encryption key and a decryption key as a common key.

There is also a variety of algorithms adopted in the common-key encryption method. An encryption method adopts one of the algorithms. In accordance with this encryption method, a plurality of keys is generated with a common key used as a base and the generated keys are used in carrying out an encryption process. As a method for generating the keys, a method using a round function is adopted. To put it in detail, in accordance with this key generation method, the round function is applied to a common key to generate a new key on the basis of the output value. Then, the round function is applied to the new key to generate another key. Subsequently, the round function is applied to the other key to generate a further key. Then, the round function is applied to the further key to generate a still further key. This procedure repeating the operation to generate a key results in a plurality of keys. A representative algorithm for generating a plurality of keys as described above is referred to as a common-key block encryption method.

The common-key block encryption processing algorithm can be divided mainly into a round function part and a key-scheduling part. Conventionally, in order to secure safety against attacks related to a key or the like, an designer of encryption method is required to design a key-scheduling part with great caution in designing a common-key block encryption method so that a simple relation among round functions is not established.

As an encryption method designed on the basis of such a guiding principle, Toshiba has proposed a common-key block encryption method called Hierocrypt. For details of the Hierocrypt common-key block encryption method, refers to, for example, a reference authored by K. Ohkuma et al. with a title of "The Block Cipher Hierocrypt," Selected Areas in Cryptography, LNCS 2012, pp. 72-88, 2000. The key-scheduling part of the Hierocrypt algorithm has a repetitive structure called a Feistel structure. A linear transformation part forming the right half of the Feistel structure tries an operation to avoid an attack related to a key by carrying out an XOR addition process on round-dependent constants.

As a matter of fact, however, in the year of 2001, Furuya et al. discovered the fact that a linear relation among round keys is established. The fact that a linear relation among round keys is established was not expected by the creator of the Hierocypt algorithm. For details of the discovery made by Furuya et al., refer to, for example, a reference authored by S. Furuya and V. Rijmen with a title of "Observations on Hierocrypt-3/L1 Key-scheduling Algorithms," Second NESSIE workshop, 2001.

In accordance with a method developed by Furuya et al. as described in the above reference, however, an equation expressing a linear relation among round keys is derived by combining algorithms of the key-scheduling part of the Hierocrypt method on a trial-and-error basis. Thus, there is no assurance that the discovered equations are all comprehended. In addition, with the trial-and-error basis, the difficulty in finding a relation equation increases in case the key scheduling becomes more complicated.

SUMMARY OF THE INVENTION

It is thus an object of the present invention addressing the problems described above to provide an encryption level indicator calculation method that is capable of comprehending all linear equations expressing relations among round keys in a common-key block encryption method without regard to the complexity of key scheduling, and capable of evaluating the encryption level of the common-key block encryption method on the basis of a discovered linear-relation equation, as well as provide a computer program implementing the encryption level indicator calculation method.

In accordance with a first aspect of the present invention, there is provided an encryption level indicator calculation method based on an encryption processing algorithm and composed of:

a step of setting a common key block encryption processing algorithm, which is to serve as the encryption processing algorithm to be used as the base of the encryption level indicator calculation method, has a key-scheduling part comprising a linear transformation part and a non-linear transformation part and includes:

a sub-step of generating initial values U_i (where i = 1, 2 and so on) from a master key;

a sub-step of calculating intermediate values $Z_i^{(0)}$ (where i = 1, 2 and so on) from the initial values U_i (where i = 1, 2 and so on);

a plurality of sub-steps of calculating intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on) from intermediate values $Z_i^{(r-1)}$ (where i = 1, 2 and so on);

a sub-step of calculating the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and the initial values U_i (where i = 1, 2 and so on); and

a sub-step of calculating round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r =

1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of eliminating the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) serving as variables so that the round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) can be expressed as a linear combination of the initial values U_i (where i = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of transforming the linear combination into a simultaneous linear equation completing transposition of terms and, thus, consisting of only terms of the initial values U_i (where i = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) on the right-hand side of the equation;

a step of transforming the simultaneous linear equation into a matricial equation;

a step of multiplying both the left-hand and right-hand sides of the matricial equation by a row-deform unitary matrix deforming a matrix on the right-hand side of the matricial equation obtained as a result of transformation into a step matrix from the left;

a step of creating a new matrix consisting of lowest N rows of a matrix on the left-hand side of the matricial equation obtained as a result of transformation where N is a number obtained as a result of subtracting the rank value of the step matrix from the number of rows in the step matrix; and

a step of finding N linear-relation equations by multiplying a column vector consisting of the round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) as elements by the new matrix generated at the preceding step,

where:

symbol U_i (where i = 1, 2 and so on) denotes an initial value of the key-scheduling part;

symbol $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an intermediate value of the key-scheduling part;

symbol $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an output of the non-linear transformation part; and

symbol $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes a round key calculated from the intermediate values Z_i (where i = 1, 2 and so on).

In accordance with a second aspect of the present invention, there is provided a program to be executed as a computer program in carrying out an encryption level indicator calculation process based on an encryption processing algorithm and composed of:

a step of setting a common key block encryption processing algorithm, which is to serve as the encryption processing algorithm to be used as the base of the encryption level indicator calculation method and includes:

a sub-step of generating initial values U_i (where i = 1, 2 and so on) from a master key;

a sub-step of calculating intermediate values $Z_i^{(0)}$ (where i = 1, 2 and so on) from the initial values U_i (where i = 1, 2 and so on);

a plurality of sub-steps of calculating intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on) from intermediate values $Z_i^{(r-1)}$ (where i = 1, 2 and so on);

a sub-step of calculating the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and the initial values U_i (where i = 1, 2 and so on); and

a sub-step of calculating round keys $K_i^{(r)}$ (where i

= 1, 2 and so on and r = 1, 2 and so on) from the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of eliminating the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) serving as variables so that the round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) can be expressed as a linear combination of the initial values U_i (where i = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of transforming the linear combination into a simultaneous linear equation completing transposition of terms and, thus, consisting of only terms of the initial values U_i (where i = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) on the right-hand side of the equation;

a step of transforming the simultaneous linear equation into a matricial equation;

a step of multiplying both the left-hand and right-hand sides of the matricial equation by a row-deform unitary matrix deforming a matrix on the right-hand side of the matricial equation obtained as a result of transformation into a step matrix from the left;

a step of creating a new matrix consisting of lowest N rows of a matrix on the left-hand side of the matricial equation obtained as a result of transformation where N is a number obtained as a result of subtracting the rank value of the step matrix from the number of rows in the step matrix; and

a step of finding N linear-relation equations by multiplying a column vector consisting of the round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) as elements by the new matrix generated at the preceding step,

where:

symbol U_i (where i = 1, 2 and so on) denotes an initial value of the key-scheduling part;

symbol $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an intermediate value of the key-scheduling part;

symbol $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an output of the non-linear transformation part; and

symbol $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes a round key calculated from the intermediate values Z_i (where i = 1, 2 and so on).

In accordance with the configuration of the present invention, it is possible to comprehend all equations expressing relations among round keys in a common-key block encryption method without regard to the complexity of key scheduling and evaluate the encryption level of the common-key block encryption method on the basis of a discovered linear-relation equation.

In addition, in accordance with the configuration of the present invention, by expressing the key-scheduling part algorithm, which is one of encryption processing algorithms, in terms of equations represented by vectors and a matrix and by eliminating non-linear transformation output values and initial values from the matrix-based equation through use of unitary transformation, it is possible to find all linear-relation equations expressing relations among round keys.

It is to be noted that the computer program provided by the present invention is a computer program that can be presented to for example a general-purpose computer system, which is capable of executing various kinds of program code, by being recorded on a recording medium in a computer-readable form or by way of communication media such as a network also in a computer-readable form. Examples of the recording medium are a CD, an FD and an MO disc. Since the computer program is presented to the computer system in a computer-readable form, the computer system is capable of carrying out a process according to the program.

The other objects, characteristics and merits of the present invention will probably become apparent from later detailed explanations of embodiments of the present invention with reference to diagrams. It is to be noted that the technical term 'system' used in this specification means a logical group configuration of a plurality of apparatus, which is not necessarily put in the same case.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 shows a flowchart referred to in explanation of an encryption level indicator calculation procedure according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The encryption level indicator calculation method provided by the present invention is explained in detail as follows. First of all, an outline of a procedure of an encryption level indicator calculation process is explained by referring to a flowchart shown in Fig. 1. After that, embodiments implementing the encryption level indicator calculation process provided by the present invention are described by giving a plurality of concrete common-key block encryption processing algorithms as examples.

[Outline of the Encryption level Indicator Calculation Process]

Fig. 1 shows a flowchart representing the encryption level indicator calculation process provided by the present invention. An outline of each processing step in the flowchart is explained as follows.

The flowchart begins with a step S101 to set an encryption processing algorithm to be used as the base of the encryption level indicator calculation method. In this case, the encryption processing algorithm to be used as the base of the encryption level indicator calculation method is a common key block encryption processing algorithm.

To put it concretely, as the encryption processing algorithm to be used as the base of the encryption level indicator calculation method, the processing at this step

S101 sets a common key block encryption processing algorithm including a key-scheduling part, which comprises a linear conversion part and a non-linear transformation part, and having:

a step of generating initial values U_i (where i = 1, 2 and so on) from a master key;

a step of calculating intermediate values $Z_i^{(0)}$ (where i = 1, 2 and so on) from the initial values U_i (where i = 1, 2 and so on);

a plurality of steps of calculating intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on) from intermediate values $Z_i^{(r-1)}$ (where i = 1, 2 and so on);

a step of calculating the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and the initial values U_i (where i = 1, 2 and so on); and

a step of calculating round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on), where:

symbol U_i (where i = 1, 2 and so on) denotes an initial value of the key-scheduling part;

symbol $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an intermediate values of the key-scheduling part;

symbol $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an output of the non-linear transformation part; and

symbol $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes a round key calculated from the intermediate values Z_i (where i = 1, 2 and so on).

Then, at the next step S102, intermediate variables of the common-key block encryption processing algorithm set at the step S101 are eliminated. To put it concretely, the processing carried out at the step S102 eliminates the intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) so that the round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) can be expressed as a linear combination of the initial values U_i (where i = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on). The concrete example of the processing will be described later.

Then, at the next step S103, a variable transposition process is carried out. To put it concretely, the processing carried out at the step S103 transforms the expression of the linear combination into a simultaneous linear equation completing transposition of terms and, thus, consisting of only terms of the initial values U_i (where i = 1, 2 and so on) and the non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on). The concrete example of the processing will be described later.

Then, at the next step S104, a matricial-equation transformation process is carried out. The matricial-equation transformation process is a process to transform the simultaneous linear equation into a matricial equation. The matricial-equation transformation process will be explained in concrete terms later.

Then, at the next step S105, a unitary transformation process is carried out. To put it in detail, both the left-hand and right-hand sides of the matricial equation are multiplied by a row-deform unitary matrix deforming a matrix on the right-hand side of the matricial equation obtained as a result of transformation into a step matrix from the left. An embodiment of the unitary transformation process will be described later.

Then, at the next step S106, a small-matrix selection process is carried out. To put it in detail, the small-matrix selection process is a process to create a new matrix consisting of lowest N rows of a matrix on the left-hand side of the matricial equation obtained as a result of transformation where N is a number obtained as a result of subtracting the rank value of the step matrix from the number of rows in the step matrix. An embodiment of the small-matrix selection process will be described later.

Then, at the next step S107, a linear-relation equation generation process is carried out. To put it in detail, the linear-relation equation generation process is a process to find N linear-relation equations by multiplying a column vector consisting of the round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) as elements by the new matrix generated at the preceding step S106. An embodiment of the linear-relation equation generation process will be described later.

The number (N) of linear-relation equations found in the process carried out at the step S107 is the encryption level indicator of the common-key block encryption algorithm set at the step S101. The processing represented by the flowchart described above is executed as a process to find the value of N, which is number of linear-relation equations comprehensively including equations representing linear relations among round keys of the common-key block encryption algorithm set at the step S101. The larger the number (N) of linear-relation equations, the smaller the encryption level. Conversely speaking, the smaller the number (N) of linear-relation equations, the larger the encryption level. Thus, the number (N) of linear-relation equations found by carrying out the processing represented by the flowchart shown in Fig. 1 can be used as the encryption level indicator of the common-key block encryption algorithm.

In accordance with the processing according to the processing procedure represented by the flowchart shown in Fig. 1, the key-scheduling part algorithm, which is one of encryption algorithms, is expressed by a matricial equation represented by vectors and a matrix. By eliminating non-linear transformation output values and initial values from the matricial equation through a unitary transformation process, all equations of linear relations among round keys can be found.

[First Embodiment of Encryption level Indicator Calculation Process]

As a first embodiment of the encryption level indicator calculation process provided by the present invention, a typical process of applying an encryption level evaluation method provided by the present invention to 'Hierocrypt-L1' is explained in detail. 'Hierocrypt-L1' is the name of a block encryption process proposed by Toshiba. The 'Hierocrypt-L1' block encryption process is a common-key block encryption process with a block length of 64 bits and a key length of 128 bits.

First of all, the step S101 of the flowchart shown in Fig. 1 is explained. As described earlier, at this step, an encryption processing algorithm is set. This step is executed as a process to set the 'Hierocrypt-L1' block encryption algorithm proposed by Toshiba.

Let symbol On denote a null matrix consisting of n rows and n columns whereas symbol In denote a unit matrix consisting of n rows and n columns. In this case, a matrix P16 is defined as follows:

[formula 1]

$$P16 = \begin{pmatrix} I2 & O2 & I2 & O2 \\ O2 & I2 & O2 & I2 \\ O2 & I2 & I2 & I2 \\ I2 & O2 & I2 & I2 \end{pmatrix}$$

Let symbol P16I denote the inverse matrix of the matrix P16. Next, matrices M5 and MB are defined as follows:

[formula 2]

$$M5 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$MB = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Then, matrices M5B and MB5 are defined, being expressed in terms of the matrices M5 and MB as follows:

[formula 3]

$$M5B = \begin{pmatrix} M5 & O4 \\ O4 & MB \end{pmatrix}$$

$$MB5 = \begin{pmatrix} MB & O4 \\ O4 & M5 \end{pmatrix}$$

Next, round dependent constant vectors Gi (where i = 0, ···, 7) are defined as follows:

[formula 4]

G0 = (h01, h02, h03, h04, 0, 0, 0, 0)

G1 = (h11, h12, h13, h14, 0, 0, 0, 0)

G2 = (h21, h22, h23, h24, 0, 0, 0, 0)

G3 = (h31, h32, h33, h34, 0, 0, 0, 0)

G4 = (h41, h42, h43, h44, 0, 0, 0, 0)

G5 = (h41, h42, h43, h44, 0, 0, 0, 0)

G6 = (h31, h32, h33, h34, 0, 0, 0, 0)

G7 = (h21, h22, h23, h24, 0, 0, 0, 0)

It is to be noted that a vector HH with constants in the above equations used as elements is defined as follows:

[formula 5]

HH = (h01, h02, h03, h04, h11, h12, h13, h14, h21, h22, h23, h24, h31, h32, h33, h34, h41, h42, h43, h44,)

The actual values of the elements h01, h02, ··· and h44 are defined as follows.

[formula 6]

(h01, h01, h02, h03) = (0x5a, 0x82, 0x79, 0x99)

(h11, h11, h12, h13) = (0x6e, 0xd9, 0xeb, 0xa1)

(h21, h21, h22, h23) = (0x8f, 0x1b, 0xbc, 0xdc)

(h31, h31, h32, h33) = (0xca, 0x62, 0xc1, 0xd6)

(h41, h42, h43, h44) = (0xf7, 0xde, 0xf5, 0x8a)

Next, a vector ZZ with its elements composing the right half of a sequence of initial values of the key-scheduling part is defined as follows.

[formula 7]

ZZ = (z31, z32, z33, z34, z41, z42, z43, z44)

By using these, the right half of the key-scheduling part in the Hierocrypt-L1 common-key encryption algorithm is expressed below. It is to be noted that the operator + used in the following expressions is an additive operator in the Galois field GF(2).

[formula 8]

$Z0 = M5B*ZZ + G0$

$W0 = P16*Z0$

$Z1 = M5B*W0 + G1$

$W1 = P16*Z1$

$Z2 = M5B*W1 + G2$

$W2 = P16*Z2$

$Z3 = M5B*W2 + G4$

$W3 = P16*Z3$

$Z4 = M5B*W3 + G4$

$W5 = M5B*(Z4 + G5)$

$Z5 = P16I*W5$

$W6 = M5B*(Z5 + G6)$

$Z6 = P16I*W6$

$W7 = M5B*(Z6 + G7)$

$Z7 = P16I*W7$

Symbols Z0, Z1, Z2, Z3, Z4, Z5, Z6, Z7, W0, W1, W2, W3, W5, W6 and W7 used in the above equations form the right half of the sequence of intermediate values of the key-scheduling part.

Next, these intermediate values are expressed by being split in accordance with the following equations.

[formula 9]

$Zn = Zn_3 || ZN_4$

$Wn = Wn_1 || WN_2$

Symbol || used in the above equations denotes a concatenation of vectors.

Next, let non-linear transformation part outputs of rounds be V0, V1, V2, V3, V4, V5, V6 and V7. Each of the outputs is a vector consisting of four elements as follows.

[formula 10]

$V0 = (v01, v02, v03, v04)$

$V1 = (v11, v12, v13, v14)$

$V2 = (v21, v22, v23, v24)$

$V3 = (v31, v32, v33, v34)$

$V4 = (v41, v42, v43, v44)$

$V5 = (v51, v52, v53, v54)$

$V6 = (v61, v62, v63, v64)$

$V7 = (v71, v72, v73, v74)$

Here, vectors Z_1 and Z_2 are set as follows.

[formula 11]

$Z_1 = (z11, z12, z13, z14)$

$Z_2 = (z21, z22, z23, z24)$

With the vectors Z_1 and Z_2 set as described above, the left half of the key-scheduling part in the

Hierocrypt-L1 common-key encryption algorithm is expressed as follows.

[formula 12]

$Z0_1 = Z_2$

$Z0_2 = Z_1 + V0$

$Z1_1 = Z0_2$

$Z1_2 = Z0_1 + V1$

$Z2_1 = Z1_2$

$Z2_2 = Z1_1 + V2$

$Z3_1 = Z2_2$

$Z3_2 = Z2_1 + V3$

$Z4_1 = Z3_2$

$Z4_2 = Z3_1 + V4$

$Z5_1 = Z4_2 + V5$

$Z5_2 = Z4_1$

$Z6_1 = Z5_2 + V6$

$Z6_2 = Z5_1$

$Z7_1 = Z5_2 + V7$

$Z7_2 = Z6_1$

Symbols $Z0_1$, $Z0_2$, $Z1_1$, $Z1_2$, $Z2_1$, $Z2_2$, $Z3_1$, $Z3_2$, $Z4_1$, $Z4_2$, $Z5_1$, $Z5_2$, $Z6_1$, $Z6_2$, $Z7_1$ and $Z7_2$ used in the above equations form the left half of the sequence of intermediate values of the key-scheduling part.

By using the intermediate values obtained as described above, round keys $K1_1$, $K1_2$, $K1_3$, $K1_4$, $K2_1$, ···, $K7_1$ and $K7_2$ are expressed as follows:

[formula 13]

$K1_1 = Z0_1 + V1$

$K1_2 = Z1_3 + V1$

$K1_3 = Z1_4 + V1$

$K1_4 = Z0_2 + z1_4$

$K2_1 = Z1_1 + V2$

$K2_2 = Z2_3 + V2$

$K2_3 = Z2_4 + V2$

$K2_4 = Z1_2 + Z2_4$

$K3_1 = Z2_1 + V3$

$K3_2 = Z3_3 + V3$

$K3_3 = Z3_4 + V3$

$K3_4 = Z2_2 + Z3_4$

$K4_1 = Z3_1 + V4$

$K4_2 = Z4_3 + V4$

$K4_3 = Z4_4 + V4$

$K5_1 = Z5_1 + Z4_3$

$K5_2 = W5_1 + V5$

$K5_3 = W5_2 + V5$

$K5_4 = Z4_1 + W5_2$

$K6_1 = Z6_1 + Z5_3$

$K6_2 = W6_1 + V6$

$K6_3 = W6_2 + V6$

$K6_4 = Z5_1 + W6_2$

$K7_1 = Z7_1 + Z6_3$

$K7_2 = W7_1 + V7$

$K7_3 = W7_2 + V7$

$K7_4 = Z6_1 + W7_2$

It is to be noted that symbols $K1_1$, $K1_2$, $K1_3$, $K1_4$, $K2_1$, •••, $K7_1$ and $K7_2$ each denote a vector consisting of four elements.

The following description explains the step S102 of carrying out a process to eliminate intermediate variables in the processing represented by the flowchart shown in Fig. 1. If the four elements of each of the vectors $K1_1$, $K1_2$, $K1_3$, $K1_4$, $K2_1$, •••, $K7_1$ and $K7_2$ are expressed by their actual values, the vectors $K1_1$, $K1_2$, $K1_3$, $K1_4$, $K2_1$, •••, $K7_1$ and $K7_2$ can be expressed as follows: [formula 14]

$$\begin{aligned}
K1_1 &= \begin{pmatrix} v11 + z21 \\ v12 + z22 \\ v13 + z23 \\ v14 + z24 \end{pmatrix} \\
K1_2 &= \begin{pmatrix} h01 + h11 + h03 + v11 + z32 + z41 \\ h01 + h02 + h12 + h04 + v12 + z33 + z42 \\ h01 + h02 + h03 + h13 + v13 + z31 + z34 + z43 \\ h02 + h04 + h14 + v14 + z31 + z44 \end{pmatrix} \\
K1_3 &= \begin{pmatrix} h02 + h04 + v11 + z31 \\ h01 + h03 + v12 + z32 \\ h02 + h03 + h04 + v13 + z32 + z41 + z33 \\ h01 + h02 + h03 + v14 + z31 + z34 + z44 \end{pmatrix} \\
K1_4 &= \begin{pmatrix} h02 + h04 + v01 + z11 + z31 \\ h01 + h03 + v02 + z12 + z32 \\ h02 + h03 + h04 + v03 + z13 + z32 + z41 + z33 \\ h01 + h02 + h03 + v04 + z31 + z14 + z34 + z44 \end{pmatrix} \\
K2_1 &= \begin{pmatrix} v01 + v21 + z11 \\ v02 + v22 + z12 \\ v03 + v23 + z13 \\ v04 + v24 + z14 \end{pmatrix} \\
K2_2 &= \begin{pmatrix} h02 + h11 + h03 + h21 + h13 + v21 + z33 + z34 + z43 \\ h11 + h03 + h12 + h04 + h22 + h14 + v22 + z31 + z41 + z33 + z42 + z34 \\ h11 + h12 + h04 + h13 + h23 + v23 + z32 + z42 + z34 + z43 \\ h01 + h02 + h12 + h14 + h24 + v24 + z32 + z33 + z42 + z34 \end{pmatrix} \\
K2_3 &= \begin{pmatrix} h01 + h12 + h14 + v21 + z31 + z33 + z42 + z44 \\ h02 + h11 + h13 + v22 + z31 + z32 + z41 + z34 + z43 \\ h02 + h12 + h13 + h14 + v23 + z31 + z32 + z41 + z42 + z34 + z43 + z44 \\ h01 + h02 + h11 + h12 + h04 + h13 + v24 + z41 + z33 + z42 + z43 + z44 \end{pmatrix} \\
K2_4 &= \begin{pmatrix} h01 + h12 + h14 + v11 + z21 + z31 + z33 + z42 + z44 \\ h02 + h11 + h13 + v12 + z22 + z31 + z32 + z41 + z34 + z43 \\ h02 + h12 + h13 + h14 + v13 + z31 + z23 + z32 + z41 + z42 + z34 + z43 + z44 \\ h01 + h02 + h11 + h12 + h04 + h13 + v14 + z41 + z24 + z33 + z42 + z43 + z44 \end{pmatrix}
\end{aligned}$$

$$K3_1 = \begin{pmatrix} v11 + v31 + z21 \\ v12 + v32 + z22 \\ v13 + v33 + z23 \\ v14 + v34 + z24 \end{pmatrix}$$

$$K3_2 = \begin{pmatrix} h01 + h03 + h12 + h21 + h04 + h13 + h31 + h23 + v31 + z41 + z42 + z34 + z43 \\ h01 + h21 + h13 + h22 + h14 + h32 + h24 + v32 + z31 + z41 + z33 + z43 \\ h01 + h02 + h21 + h22 + h14 + h23 + h33 + v33 + z32 + z41 + z33 + z34 \\ h02 + h11 + h03 + h12 + h22 + h24 + h34 + v34 + z41 + z33 + z42 + z34 + z44 \end{pmatrix}$$

$$K3_3 = \begin{pmatrix} h01 + h02 + h11 + h03 + h04 + h22 + h24 + v31 + z31 + z32 + z41 \\ h02 + h03 + h12 + h21 + h04 + h23 + v32 + z32 + z33 + z42 \\ h03 + h12 + h22 + h23 + h24 + v33 + z31 + z32 + z33 + z42 \\ h01 + h02 + h11 + h12 + h21 + h04 + h22 + h14 + h23 + v34 + z41 + z33 + z42 + z44 \end{pmatrix}$$

$$K3_4 = \begin{pmatrix} h01 + h02 + h11 + h03 + h04 + h22 + h24 + v01 + v21 + z11 + z31 + z32 + z41 \\ h02 + h03 + h12 + h21 + h04 + h23 + v02 + v22 + z12 + z32 + z33 + z42 \\ h03 + h12 + h22 + h23 + h24 + v03 + v23 + z13 + z31 + z32 + z33 + z42 \\ h01 + h02 + h11 + h12 + h21 + h04 + h22 + h14 + h23 + v04 + v24 + z14 + z41 + z33 \\ +z42 + z44 \end{pmatrix}$$

$$k4_1 = \begin{pmatrix} v01 + v21 + v41 + z11 \\ v02 + v22 + v42 + z12 \\ v03 + v23 + v43 + z13 \\ v04 + v24 + v44 + z14 \end{pmatrix}$$

$$k4_2 = \begin{pmatrix} h01 + h11 + h03 + h13 + h22 + h31 + h14 + h23 + h41 + h33 + v41 + z32 + z41 + z43 \\ h11 + h31 + h23 + h32 + h24 + h42 + h34 + v42 + z41 \\ h02 + h11 + h12 + h04 + h31 + h32 + h24 + h33 + h43 + v43 + z31 + z42 \\ h02 + h12 + h21 + h13 + h22 + h32 + h34 + h44 + v44 + z31 + z32 + z41 + z42 + z34 \\ +z43 \end{pmatrix}$$

$$k4_3 = \begin{pmatrix} h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + h32 + h34 + v41 + z31 + z42 + z34 \\ +z43 + z44 \\ h02 + h03 + h12 + h04 + h13 + h22 + h31 + h14 + h33 + v42 + z32 + z33 + z42 + z43 \\ h01 + h02 + h03 + h04 + h13 + h22 + h32 + h33 + h34 + v43 + z31 + z32 + z43 + z44 \\ h02 + h11 + h12 + h21 + h04 + h22 + h31 + h14 + h32 + h24 + h33 + v44 + z31 + z42 \\ +z44 \end{pmatrix}$$

$$k4_4 = \left(\begin{array}{l} h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + h32 + h34 + v11 + v31 + z21 + z31 \\ +z42 + z34 + z43 + z44 \\ h02 + h03 + h12 + h04 + h13 + h22 + h31 + h14 + h33 + v12 + v32 + z22 + z32 + z33 \\ +z42 + z43 \\ h01 + h02 + h03 + h04 + h13 + h22 + h32 + h33 + h34 + v13 + v33 + z31 + z23 + z32 \\ +z43 + z44 \\ h02 + h11 + h12 + h21 + h04 + h22 + h31 + h14 + h32 + h24 + h33 + v14 + v34 + z31 \\ +z24 + z42 + z44 \end{array} \right)$$

$$K5_1 = \left(\begin{array}{l} h01 + h11 + h03 + h13 + h22 + h31 + h14 + h23 + h41 + h33 + v01 + v21 + v41 + v51 \\ +z11 + z32 + z41 + z43 \\ h11 + h31 + h23 + h32 + h24 + h42 + h34 + v02 + v22 + v42 + v52 + z12 + z41 \\ h02 + h11 + h12 + h04 + h31 + h32 + h24 + h33 + h43 + v03 + v23 + v43 + v53 + z13 \\ +z31 + z42 \\ h02 + h12 + h21 + h13 + h22 + h32 + h34 + h44 + v04 + v24 + v44 + z31 + v54 + z14 \\ +z32 + z41 + z42 + z34 + z43 \end{array} \right)$$

$$K5_2 = \left(\begin{array}{l} h02 + h11 + h12 + h21 + h13 + h22 + h31 + h23 + h24 + v51 + z31 + z32 + z42 + z34 \\ +z43 \\ h01 + h02 + h03 + h12 + h04 + h13 + h22 + h14 + h23 + h32 + h24 + v52 + z31 + z32 \\ +z41 + z42 + z43 \\ h01 + h02 + h03 + h12 + h21 + h14 + h24 + h33 + v53 + z31 + z41 + z42 + z34 \\ h01 + h03 + h21 + h04 + h14 + h23 + h24 + h34 + v54 + z34 \end{array} \right)$$

$$K5_3 = \left(\begin{array}{l} h11 + h12 + h21 + h04 + h22 + h14 + h33 + v51 + z32 + z42 + z34 \\ h01 + h02 + h12 + h14 + h24 + h34 + v52 + z32 + z33 + z42 + z34 \\ h02 + h11 + h03 + h21 + h13 + h31 + v53 + z33 + z34 + z43 \\ h11 + h03 + h21 + h13 + h32 + h24 + z31 + v54 + z32 + z33 + z43 + z44 \end{array} \right)$$

$$K5_4 = \left(\begin{array}{l} h11 + h12 + h21 + h04 + h22 + h14 + h33 + v11 + v31 + z21 + z32 + z42 + z34 \\ h01 + h02 + h12 + h14 + h24 + h34 + v12 + v32 + z22 + z32 + z33 + z42 + z34 \\ h02 + h11 + h03 + h21 + h13 + h31 + v13 + v33 + z23 + z33 + z34 + z43 \\ h11 + h03 + h21 + h13 + h32 + h24 + v14 + v34 + z31 + z32 + z24 + z33 + z43 + z44 \end{array} \right)$$

$$K6_1 = \left(\begin{array}{l} h01 + h03 + h12 + h21 + h04 + h13 + h31 + h23 + v11 + v31 + v61 + z21 + z41 + z42 \\ +z34 + z43 \\ h01 + h21 + h13 + h22 + h14 + h32 + h24 + v12 + v32 + v62 + z22 + z31 + z41 + z33 \\ +z43 \\ h01 + h02 + h21 + h22 + h14 + h23 + h33 + v13 + v33 + v63 + z23 + z32 + z41 + z33 \\ +z34 \\ h02 + h11 + h03 + h12 + h22 + h24 + h34 + v14 + v34 + z41 + v64 + z24 + z33 + z42 \\ +z34 + z44 \end{array} \right)$$

$$K6_2 = \begin{pmatrix} h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + v61 + z31 + z42 + z34 + z43 + z44 \\ h02 + h03 + h12 + h04 + h13 + h22 + h14 + v62 + z32 + z33 + z42 + z43 \\ h02 + h11 + h04 + h14 + h23 + z31 + v63 + z41 + z44 \\ h11 + h04 + h13 + h14 + h24 + z32 + z41 + v64 + z34 + z43 + z44 \end{pmatrix}$$

$$K6_3 = \begin{pmatrix} h01 + h02 + h11 + h12 + h04 + h23 + v61 + z41 + z33 + z42 \\ h02 + h04 + h14 + h24 + v62 + z31 + z44 \\ h01 + h11 + h03 + h21 + v63 + z32 + z41 \\ h01 + h11 + h03 + h22 + h14 + z32 + z41 + v64 + z44 \end{pmatrix}$$

$$K6_4 = \begin{pmatrix} h01 + h02 + h11 + h12 + h04 + h23 + v01 + v21 + v41 + v51 + z11 + z41 + z33 + z42 \\ h02 + h04 + h14 + h24 + v02 + v22 + v42 + v52 + z12 + z31 + z44 \\ h01 + h11 + h03 + h21 + v03 + v23 + v43 + v53 + z13 + z32 + z41 \\ h01 + h11 + h03 + h22 + h14 + v04 + v24 + v44 + v54 + z14 + z32 + z41 + z44 \end{pmatrix}$$

$$K7_1 = \begin{pmatrix} h02 + h11 + h03 + h21 + h13 + v01 + v21 + v41 + v51 + z11 + v71 + z33 + z34 + z43 \\ h11 + h03 + h12 + h04 + h22 + h14 + v02 + v22 + v42 + v52 + z12 + z31 + v72 + z41 \\ +z33 + z42 + z34 \\ h11 + h12 + h04 + h13 + h23 + v03 + v23 + v43 + v53 + z13 + z32 + v73 + z42 + z34 \\ +z43 \\ h01 + h02 + h12 + h14 + h24 + v04 + v24 + v44 + v54 + z14 + z32 + z33 + z42 + v74 \\ +z34 \end{pmatrix}$$

$$K7_2 = \begin{pmatrix} h01 + h02 + h11 + h03 + h04 + v71 + z31 + z32 + z41 \\ h02 + h03 + h12 + h04 + v72 + z32 + z33 + z42 \\ h01 + h04 + h13 + z31 + z32 + z41 + v73 + z33 + z34 + z43 \\ h01 + h03 + h04 + h14 + v74 + z34 \end{pmatrix}$$

Then, the next step S103 is executed to carry out a variable transposition process. With the results of the vectors $K1_1$, $K1_2$, $K1_3$, $K1_4$, $K2_1$, $\cdots$, $K7_1$ and $K7_2$ used as a base, the simultaneous linear equation is transformed so as to result in equations, which each include only terms zxx and vxx on the right-hand side thereof as follows.

[formula 15]

$k1_{11} = v11 + z21$

$k1_{12} = v12 + z22$

$k1_{13} = v13 + z23$

$k1_{14} = v14 + z24$

$h01 + h11 + h03 + k1_{21} = v11 + z32 + z41$

$h01 + h02 + h12 + h04 + k1_{22} = v12 + z33 + z42$

$h01 + h02 + h03 + h13 + k1_{23} = v13 + z31 + z34 + z43$

$h02 + h04 + h14 + k1_{24} = v14 + z31 + z44$

$h02 + h04 + k1_{31} = v11 + z31$

$h01 + h03 + k1_{32} = v12 + z32$

$h02 + h03 + h04 + k1_{33} = v13 + z32 + z41 + z33$

$h01 + h02 + h03 + k1_{34} = v14 + z31 + z34 + z44$

$h02 + h04 + k1_{41} = v01 + z11 + z31$

$h01 + h03 + k1_{42} = v02 + z12 + z32$

$h02 + h03 + h04 + k1_{43} = v03 + z13 + z32 + z41 + z33$

$h01 + h02 + h03 + k1_{44} = v04 + z31 + z14 + z34 + z44$

$k2_{11} = v01 + v21 + z11$

$k2_{12} = v02 + v22 + z12$

$k2_{13} = v03 + v23 + z13$

$k2_{14} = v04 + v24 + z14$

$h02 + h11 + h03 + h21 + h13 + k2_{21} = v21 + z33 + z34 + z43$

$h11 + h03 + h12 + h04 + h22 + h14 + k2_{22} = v22 + z31 + z41 + z33 + z42 + z34$

$h11 + h12 + h04 + h13 + h23 + k2_{23} = v23 + z32 + z42 + z34 + z43$

$h01 + h02 + h12 + h14 + h24 + k2_{24} = v24 + z32 + z33 + z42 + z34$

$h01 + h12 + h14 + k2_{31} = v21 + z31 + z33 + z42 + z44$

$h02 + h11 + h13 + k2_{32} = v22 + z31 + z32 + z41 + z34 + z43$

$h02 + h12 + h13 + h14 + k2_{33} = v23 + z31 + z32 + z41 + z42 + z34 + z43 + z44$

$h01 + h02 + h11 + h12 + h04 + h13 + k2_{34} = v24 + z41 + z33 + z42 + z43 + z44$

$h01 + h12 + h14 + k2_{41} = v11 + z21 + z31 + z33 + z42 + z44$

$h02 + h11 + h13 + k2_{42} = v12 + z22 + z31 + z32 + z41 + z34 + z43$

$h02 + h12 + h13 + h14 + k2_{43} = v13 + z31 + z23 + z32 + z41 + z42 + z34 + z43 + z44$

$h01 + h02 + h11 + h12 + h04 + h13 + k2_{44} = v14 + z41 + z24 + z33 + z42 + z43 + z44$

$k3_{11} = v11 + v31 + z21$

$k3_{12} = v12 + v32 + z22$

$k3_{13} = v13 + v33 + z23$

$k3_{14} = v14 + v34 + z24$

$h01 + h03 + h12 + h21 + h04 + h13 + h31 + h23 + k3_{21} = v31 + z41 + z42 + z34 + z43$

$h01 + h21 + h13 + h22 + h14 + h32 + h24 + k3_{22} = v32 + z31 + z41 + z33 + z43$

$h01 + h02 + h21 + h22 + h14 + h23 + h33 + k3_{23} = v33 + z32 + z41 + z33 + z34$

$h02 + h11 + h03 + h12 + h22 + h24 + h34 + k3_{24} = v34 + z41 + z33 + z42 + z34 + z44$

$h01 + h02 + h11 + h03 + h04 + h22 + h24 + k3_{31} = v31 + z31 + z32 + z41$

$h02 + h03 + h12 + h21 + h04 + h23 + k3_{32} = v32 + z32 + z33 + z42$

$h03 + h12 + h22 + h23 + h24 + k3_{33} = v33 + z31 + z32 + z33 + z42$

$h01 + h02 + h11 + h12 + h21 + h04 + h22 + h14 + h23 + k3_{34} = v34 + z41 + z33 + z42 + z44$

$h01 + h02 + h11 + h03 + h04 + h22 + h24 + k3_{41} = v01 + v21 + z11 + z31 + z32 + z41$

$h02 + h03 + h12 + h21 + h04 + h23 + k3_{42} = v02 + v22 + z12 + z32 + z33 + z42$

$h03+h12+h22+h23+h24+k3_{43} = v03+v23+z13+z31+z32+z33+z42$

$h01 + h02 + h11 + h12 + h21 + h04 + h22 + h14 + h23 + k3_{44} = v04 + v24 + z14 + z41 + z33 + z42 + z44$

$k4_{11} = v01 + v21 + v41 + z11$

$k4_{12} = v02 + v22 + v42 + z12$

$k4_{13} = v03 + v23 + v43 + z13$

$k4_{14} = v04 + v24 + v44 + z14$

$h01 + h11 + h03 + h13 + h22 + h31 + h14 + h23 + h41 + h33 + k4_{21} = v41 + z32 + z41 + z43$

$h11 + h31 + h23 + h32 + h24 + h42 + h34 + k4_{22} = v42 + z41$

$h02+h11+h12+h04+h31+h32+h24+h33+h43+k4_{23} = v43+z31+z42$

$h02 + h12 + h21 + h13 + h22 + h32 + h34 + h44 + k4_{24} = v44 + z31 + z32 + z41 + z42 + z34 + z43$

$h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + h32 + h34 + k4_{31} = v41 + z31 + z42 + z34 + z43 + z44$

$h02 + h03 + h12 + h04 + h13 + h22 + h31 + h14 + h33 + k4_{32} = v42 + z32 + z33 + z42 + z43$

$h01 + h02 + h03 + h04 + h13 + h22 + h32 + h33 + h34 + k4_{33} = v43 + z31 + z32 + z43 + z44$

$h02+h11+h12+h21+h04+h22+h31+h14+h32+h24+h33+k4_{34} = v44 + z31 + z42 + z44$

$h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + h32 + h34 + k4_{41} = v11 + v31 + z21 + z31 + z42 + z34 + z43 + z44$

$h02 + h03 + h12 + h04 + h13 + h22 + h31 + h14 + h33 + k4_{42} = v12 + v32 + z22 + z32 + z33 + z42 + z43$

$h01 + h02 + h03 + h04 + h13 + h22 + h32 + h33 + h34 + k4_{43} = v13 + v33 + z31 + z23 + z32 + z43 + z44$

$h02+h11+h12+h21+h04+h22+h31+h14+h32+h24+h33+k4_{44} = v14 + v34 + z31 + z24 + z42 + z44$

$h01 + h11 + h03 + h13 + h22 + h31 + h14 + h23 + h41 + h33 + k5_{11} = v01 + v21 + v41 + v51 + z11 + z32 + z41 + z43$

$h11 + h31 + h23 + h32 + h24 + h42 + h34 + k5_{12} = v02 + v22 + v42 + v52 + z12 + z41$

$h02 + h11 + h12 + h04 + h31 + h32 + h24 + h33 + h43 + k5_{13} = v03 + v23 + v43 + v53 + z13 + z31 + z42$

$h02 + h12 + h21 + h13 + h22 + h32 + h34 + h44 + k5_{14} = v04 + v24 + v44 + z31 + v54 + z14 + z32 + z41 + z42 + z34 + z43$

$h02 + h11 + h12 + h21 + h13 + h22 + h31 + h23 + h24 + k5_{21} = v51 + z31 + z32 + z42 + z34 + z43$

$h01 + h02 + h03 + h12 + h04 + h13 + h22 + h14 + h23 + h32 + h24 + k5_{22} = v52 + z31 + z32 + z41 + z42 + z43$

$h01 + h02 + h03 + h12 + h21 + h14 + h24 + h33 + k5_{23} = v53 + z31 + z41 + z42 + z34$

$h01 + h03 + h21 + h04 + h14 + h23 + h24 + h34 + k5_{24} = v54 + z34$

$h11 + h12 + h21 + h04 + h22 + h14 + h33 + k5_{31} = v51 + z32 + z42 + z34$

$h01 + h02 + h12 + h14 + h24 + h34 + k5_{32} = v52 + z32 + z33 + z42 + z34$

$h02 + h11 + h03 + h21 + h13 + h31 + k5_{33} = v53 + z33 + z34 + z43$

$h11 + h03 + h21 + h13 + h32 + h24 + z31 + k5_{34} = v54 + z32 + z33 + z43 + z44$

$h11 + h12 + h21 + h04 + h22 + h14 + h33 + k5_{41} = v11 + v31 + z21 + z32 + z42 + z34$

$h01 + h02 + h12 + h14 + h24 + h34 + k5_{42} = v12 + v32 + z22 + z32 + z33 + z42 + z34$

$h02 + h11 + h03 + h21 + h13 + h31 + k5_{43} = v13 + v33 + z23 + z33 + z34 + z43$

$h11 + h03 + h21 + h13 + h32 + h24 + k5_{44} = v14 + v34 + z31 + z32 + z24 + z33 + z43 + z44$

$h01 + h03 + h12 + h21 + h04 + h13 + h31 + h23 + k6_{11} = v11 + v31 + v61 + z21 + z41 + z42 + z34 + z43$

$h01 + h21 + h13 + h22 + h14 + h32 + h24 + k6_{12} = v12 + v32 + v62 + z22 + z31 + z41 + z33 + z43$

$h01 + h02 + h21 + h22 + h14 + h23 + h33 + k6_{13} = v13 + v33 + v63 + z23 + z32 + z41 + z33 + z34$

$h02 + h11 + h03 + h12 + h22 + h24 + h34 + k6_{14} = v14 + v34 + z41 + v64 + z24 + z33 + z42 + z34 + z44$

$h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + k6_{21} = v61 + z31 + z42 + z34 + z43 + z44$

$h02 + h03 + h12 + h04 + h13 + h22 + h14 + k6_{22} = v62 + z32 + z33 + z42 + z43$

$h02 + h11 + h04 + h14 + h23 + z31 + k6_{23} = v63 + z41 + z44$

$h11 + h04 + h13 + h14 + h24 + z32 + z41 + k6_{24} = v64 + z34 + z43 + z44$

$h01 + h02 + h11 + h12 + h04 + h23 + k6_{31} = v61 + z41 + z33 + z42$

$h02 + h04 + h14 + h24 + k6_{32} = v62 + z31 + z44$

$h01 + h11 + h03 + h21 + k6_{33} = v63 + z32 + z41$

$h01 + h11 + h03 + h22 + h14 + z32 + z41 + k6_{34} = v64 + z44$

$h01 + h02 + h11 + h12 + h04 + h23 + k6_{41} = v01 + v21 + v41 + v51 + z11 + z41 + z33 + z42$

$h02 + h04 + h14 + h24 + k6_{42} = v02 + v22 + v42 + v52 + z12 + z31 + z44$

$h01 + h11 + h03 + h21 + k6_{43} = v03 + v23 + v43 + v53 + z13 + z32 + z41$

$h01 + h11 + h03 + h22 + h14 + k6_{44} = v04 + v24 + v44 + v54 + z14 + z32 + z41 + z44$

$h02+h11+h03+h21+h13+k7_{11}=v01+v21+v41+v51+z11+v71+z33+z34+z43$

$h11+h03+h12+h04+h22+h14+k7_{12}=v02+v22+v42+v52+z12+z31+v72+z41+z33+z42+z34$

$h11+h12+h04+h13+h23+k7_{13}=v03+v23+v43+v53+z13+z32+v73+z42+z34+z43$

$h01+h02+h12+h14+h24+k7_{14}=v04+v24+v44+v54+z14+z32+z33+z42+v74+z34$

$h01+h02+h11+h03+h04+k7_{21}=v71+z31+z32+z41$

$h02+h03+h12+h04+k7_{22}=v72+z32+z33+z42$

$h01+h04+h13+z31+z32+z41+k7_{23}=v73+z33+z34+z43$

$h01+h03+h04+h14+k7_{24}=v74+z34$

Then, the next step S104 is executed to carry out a matricial-equation transformation process. In this process, vectors K, H, U and V are set as follows.

[formula 16]

$K = (k1_{11},\ k1_{12},\ \cdots,\ k7_{24})$

$H = (h01,\ h02,\ \cdots,\ h44)$

$U = (z01,\ z02,\ \cdots,\ z44)$

$V = (v01,\ v02,\ \cdots,\ v74)$

With the vectors K, H, U and V set as expressed by the above equations, the simultaneous linear equation can be transformed into the following matricial equation.

[formula 17]

$$M_{KH}\begin{pmatrix} {}^{t}K \\ {}^{t}H \end{pmatrix} = M_{UV}\begin{pmatrix} {}^{t}U \\ {}^{t}V \end{pmatrix}$$

It is to be noted that, in the above equation, symbols M_{KH} and M_{UV} each denote a GF(2) matrix comprising coefficients of the simultaneous linear equation described above.

Then, the next step S105 is executed to carry out a unitary transformation process.

Let symbol N_r denote the rank value of the matrix M_{UV} as follows:

[formula 18]

$$\mathrm{rank}\ (M_{UV}) = N_r$$

Then, let symbol N_m denote the number of rows composing the matrix M_{UV}. By multiplying both the left-hand and right-hand sides of the matricial equation by a row-deform unitary matrix Q from the left, the matrix M_{UV} can be deformed into a step matrix. In this process, a small matrix consisting of $(N_m - N_r)$ lowest rows of the matrix QM_{UV} becomes a null matrix.

Then, the next step S106 is executed to carry out a small-matrix selection process. Let symbol M^*_{KH} denote a small matrix consisting of $(N_m - N_r)$ lowest rows of the matrix QM_{KH}. In this case, the small matrix M^*_{KH} becomes a null matrix (O) as expressed by the following equation.

[formula 19]

$$M^*_{KH} = O$$

Then, the next step S107 is executed to carry out a linear-relation equation generation process. This matricial equation is transformed into linear-relation equations, which are each associated with a row. Then, actual values are substituted for h01, h02, ··· and h44 to obtain the following relation equations:

[formula 20]

$$0xc7 = k1_{11} + k1_{21} + k1_{22} + k1_{24} + k1_{31} + k1_{32} + k1_{34} + k1_{42} + k1_{44} + k2_{12} + k2_{14} + k2_{22} + k2_{24} + k2_{41}$$

$$0x33 = k1_{12} + k1_{21} + k1_{22} + k1_{23} + k1_{31} + k1_{32} + k1_{33} + k1_{41} + k1_{43} + k2_{11} + k2_{13} + k2_{21} + k2_{23} + k2_{42}$$

$0x48 = k1_{13} + k1_{22} + k1_{24} + k1_{32} + k1_{34} + k1_{41} + k1_{42} + k1_{44} + k2_{11} + k2_{12} + k2_{14} + k2_{21} + k2_{22} + k2_{24} + k2_{43}$

$0xef = k1_{14} + k1_{21} + k1_{22} + k1_{23} + k1_{24} + k1_{31} + k1_{32} + k1_{33} + k1_{34} + k1_{41} + k1_{43} + k1_{44} + k2_{11} + k2_{13} + k2_{14} + k2_{21} + k2_{23} + k2_{24} + k2_{44}$

$0xc7 = k1_{21} + k1_{31} + k2_{11} + k3_{41}$

$0x33 = k1_{22} + k1_{32} + k2_{12} + k3_{42}$

$0x00 = k1_{23} + k1_{33} + k1_{41} + k2_{12} + k2_{13} + k2_{21} + k3_{41} + k3_{42} + k3_{43}$

$0xd4 = k1_{24} + k1_{34} + k1_{43} + k2_{11} + k2_{12} + k2_{13} + k2_{23} + k3_{42} + k4_{11} + k4_{21}$

$0xc7 = k1_{41} + k1_{42} + k2_{21} + k2_{22} + k3_{42} + k3_{43} + k4_{11} + k4_{13} + k4_{21} + k4_{23}$

$0x74 = k1_{42} + k1_{43} + k2_{11} + k2_{12} + k2_{22} + k2_{23} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{21} + k4_{22}$

$0x65 = k1_{43} + k2_{12} + k2_{14} + k2_{23} + k3_{42} + k4_{13} + k4_{14} + k4_{23} + k4_{24}$

$0x33 = k1_{44} + k2_{11} + k2_{24} + k3_{41} + k3_{44}$

$0x8a = k2_{11} + k2_{12} + k3_{42} + k3_{44} + k4_{11} + k4_{14} + k4_{24} + k4_{31}$

$0xf7 = k2_{12} + k2_{13} + k3_{41} + k3_{43} + k4_{11} + k4_{12} + k4_{21} + k4_{32}$

$0x29 = k2_{13} + k2_{14} + k3_{41} + k3_{42} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{22} + k4_{33}$

$0xa1 = k2_{14} + k3_{41} + k3_{44} + k4_{11} + k4_{22} + k4_{23} + k4_{24} + k4_{31} + k4_{32} + k4_{33} + k4_{34}$

$0x41 = k2_{21} + k2_{31} + k3_{41} + k3_{43} + k3_{44} + k4_{11} + k4_{13} + k4_{14} + k4_{23} + k4_{31} + k4_{34}$

$0x74 = k2_{22} + k2_{32} + k3_{41} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{13} + k4_{23} + k4_{24} + k4_{31} + k4_{32} + k4_{34}$

$0xf4 = k2_{23} + k2_{33} + k3_{41} + k3_{42} + k3_{43} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{24} + k4_{31} + k4_{32} + k4_{33}$

$0x57 = k2_{24} + k2_{34} + k4_{24} + k4_{34}$

$0xf6 = k2_{41} + k3_{11} + k3_{21} + k3_{41} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{34}$

$0x7c = k2_{42} + k3_{12} + k3_{22} + k3_{42} + k4_{12} + k4_{22} + k4_{23} + k4_{24} + k4_{33} + k4_{34}$

$0x43 = k2_{43} + k3_{13} + k3_{23} + k3_{41} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{32} + k4_{33}$

$0x5f = k2_{44} + k3_{14} + k3_{24} + k3_{43} + k4_{13} + k4_{22} + k4_{24} + k4_{32} + k4_{33} + k4_{34}$

$0x7d = k3_{11} + k3_{41} + k3_{42} + k3_{43} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{21} + k4_{24} + k4_{32} + k4_{33} + k5_{41}$

$0x2b = k3_{12} + k3_{41} + k3_{42} + k4_{11} + k4_{12} + k4_{22} + k4_{23} + k4_{31} + k4_{33} + k5_{42}$

$0x02 = k3_{13} + k3_{44} + k4_{14} + k4_{21} + k4_{23} + k4_{31} + k4_{33} + k4_{34} + k5_{43}$

$0xdc = k3_{14} + k3_{42} + k3_{43} + k3_{44} + k4_{12} + k4_{13} + k4_{14} + k4_{22} + k4_{33} + k4_{34} + k5_{44}$

$0x8a = k3_{21} + k3_{31} + k3_{42} + k3_{43} + k3_{44} + k4_{12} + k4_{13} + k4_{14} + k4_{24} + k4_{32} + k4_{33}$

$0x7f = k3_{22} + k3_{32} + k3_{41} + k3_{42} + k3_{43} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{23} + k4_{24} + k4_{31} + k4_{32}$

$0x88 = k3_{23} + k3_{33} + k3_{41} + k3_{42} + k4_{11} + k4_{12} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{33} + k4_{34}$

$0x54 = k3_{24} + k3_{34} + k3_{42} + k3_{43} + k4_{12} + k4_{13} + k4_{22} + k4_{24} + k4_{33} + k4_{34}$

$0x7f = k3_{41} + k3_{42} + k4_{12} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{33} + k4_{34} + k5_{11} + k5_{21}$

$0x7f = k3_{42} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{24} + k4_{31} + k4_{32} + k4_{34} + k5_{11} + k5_{13} + k5_{21} + k5_{23}$

$0x8a = k3_{43} + k3_{44} + k4_{11} + k4_{13} + k4_{21} + k4_{31} + k4_{33} + k4_{34} + k5_{11} + k5_{14} + k5_{21} + k5_{24}$

$0x00 = k3_{44} + k4_{12} + k4_{14} + k4_{22} + k4_{32} + k4_{34} + k5_{12} + k5_{22}$

$0xf7 = k4_{11} + k4_{13} + k4_{23} + k4_{33} + k4_{41} + k5_{11} + k5_{13} + k5_{21} + k5_{23} + k5_{41}$

$0x29 = k4_{12} + k4_{13} + k4_{14} + k4_{21} + k4_{23} + k4_{24} + k4_{31} + k4_{33} + k4_{34} + k4_{41} + k4_{42} + k5_{12} + k5_{13} + k5_{14} + k5_{22} + k5_{23} + k5_{24} + k5_{41} + k5_{42}$

$0x2b = k4_{13} + k4_{14} + k4_{22} + k4_{24} + k4_{32} + k4_{34} + k4_{42} + k4_{43} + k5_{13} + k5_{14} + k5_{23} + k5_{24} + k5_{42} + k5_{43}$

$0x88 = k4_{14} + k4_{21} + k4_{23} + k4_{31} + k4_{33} + k4_{41} + k4_{43} + k4_{44} + k5_{14} + k5_{24} + k5_{41} + k5_{43} + k5_{44}$

$0x43 = k4_{21} + k4_{31} + k5_{41} + k6_{11} + k6_{21}$

$0xc0 = k4_{22} + k4_{24} + k4_{32} + k4_{34} + k4_{41} + k4_{42} + k4_{44} + k5_{44} + k6_{11} + k6_{12} + k6_{21} + k6_{32}$

$0xcb = k4_{23} + k4_{24} + k4_{33} + k4_{34} + k4_{41} + k5_{43} + k6_{11} + k6_{13} + k6_{21} + k6_{33}$

$0x81 = k4_{24} + k4_{34} + k4_{42} + k4_{43} + k5_{43} + k6_{12} + k6_{22}$

$0x7e = k4_{41} + k5_{41} + k5_{43} + k6_{13} + k6_{23}$

$0xdd = k4_{42} + k4_{43} + k4_{44} + k5_{42} + k5_{43} + k6_{14} + k6_{24}$

$0x00 = k4_{43} + k4_{44} + k5_{43} + k6_{14} + k6_{34}$

$0x00 = k4_{44} + k5_{41} + k5_{44} + k6_{11} + k6_{31}$

$0xf7 = k5_{11} + k5_{41} + k6_{11} + k6_{31} + k6_{41}$

$0x14 = k5_{12} + k5_{41} + k5_{43} + k5_{44} + k6_{11} + k6_{13} + k6_{14} + k6_{21} + k6_{23} + k6_{34} + k6_{42}$

$0x23 = k5_{13} + k5_{41} + k5_{42} + k6_{11} + k6_{12} + k6_{22} + k6_{24} + k6_{31} + k6_{34} + k6_{43}$

$0x8a = k5_{14} + k5_{44} + k6_{14} + k6_{34} + k6_{44}$

$0xb4 = k5_{21} + k5_{31} + k5_{41} + k5_{42} + k6_{11} + k6_{12} + k6_{21} + k6_{32}$

$0x0b = k5_{22} + k5_{32} + k5_{42} + k5_{43} + k6_{12} + k6_{13} + k6_{22} + k6_{33}$

$0x00 = k5_{23} + k5_{33} + k5_{41} + k5_{42} + k5_{44} + k6_{11} + k6_{12} + k6_{14} + k6_{31} + k6_{32} + k6_{34}$

$0x00 = k5_{24} + k5_{34} + k5_{41} + k5_{43} + k5_{44} + k6_{11} + k6_{13} + k6_{14} + k6_{31} + k6_{33} + k6_{34}$

$0xc7 = k5_{41} + k5_{42} + k5_{43} + k5_{44} + k6_{11} + k6_{12} + k6_{13} + k6_{14} + k6_{21} + k6_{23} + k6_{32} + k6_{34} + k6_{41} + k7_{11} + k7_{21}$

$0xfc = k5_{42} + k6_{12} + k6_{21} + k6_{31} + k6_{32} + k6_{43} + k7_{13} + k7_{23}$

$0x18 = k5_{43} + k5_{44} + k6_{13} + k6_{14} + k6_{21} + k6_{22} + k6_{31} + k6_{32} + k6_{33} + k6_{34} + k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{23} + k7_{24}$

$0xf4 = k6_{21} + k6_{22} + k6_{23} + k6_{24} + k6_{31} + k6_{32} + k6_{33} + k6_{34} + k6_{41} + k6_{42} + k7_{11} + k7_{12} + k7_{21} + k7_{22}$

Here, the following equation holds true.

[formula 21]

$$\mathrm{rank}(M^{*}_{KH}) = N_m - N_r$$

Thus, the above 60 linear-relation equations are linear-relation equations independent of each other. It is therefore obvious that $(2^{60} - 1)$ linear-relation equations obtained from linear concatenation of any of the 60 equations on the GF(2) hold true. If the number of such linear-relation equations is large, it is feared that a new attack that the designer of the encryption method is not aware of is brought about. For this reason, the total number of linear-relation equations obtained by adoption of the method described above can be used as an indicator for the evaluation of the encryption level.

[Second Embodiment of Encryption level Indicator Calculation Process]

As a second embodiment of the encryption level indicator calculation process provided by the present invention, a typical process of applying an encryption level evaluation method provided by the present invention to 'Hierocrypt-3' is explained in detail. 'Hierocrypt-3' is the name of an AES-compatible block encryption process proposed by Toshiba. The 'Hierocrypt-3' block encryption process is a common-key block encryption process with a block length of 128 bits and a key length of 128, 192 or 256 bits. A typical encryption process explained below is a process with a key length of 256 bits.

First of all, the step S101 of the flowchart shown in Fig. 1 is explained. As described earlier, at this step, an encryption processing algorithm is set. This step is executed as a process to set the 'Hierocrypt-3' block encryption algorithm proposed by Toshiba.

First of all, a matrix P32 is defined as follows:
[formula 22]

$$P32 = \begin{pmatrix} I4 & O4 & I4 & O4 \\ O4 & I4 & O4 & I4 \\ O4 & I4 & I4 & I4 \\ I4 & O4 & I4 & I4 \end{pmatrix}$$

Let symbol P32I denote the inverse matrix of the matrix P32. Next, matrices M51, M52, MB1 and MB2 are defined as follows:

[formula 23]

$$M51 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$M52 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$MB1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$MB2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Then, matrices M51, M52, MB1 and MB2 are defined, being expressed in terms of the matrices M5 and MB as follows:

[formula 24]

$$M5 = \begin{pmatrix} M51 & O4 & O4 & O4 \\ O4 & M52 & O4 & O4 \\ O4 & O4 & M51 & O4 \\ O4 & O4 & O4 & M52 \end{pmatrix}$$

$$MB = \begin{pmatrix} MB1 & O4 & O4 & O4 \\ O4 & MB2 & O4 & O4 \\ O4 & O4 & MB1 & O4 \\ O4 & O4 & O4 & MB2 \end{pmatrix}$$

Next, round dependent constant vectors Gi (where i = 0, $\cdots$, 9) are defined as follows:

[formula 25]

$$\begin{aligned}
G0 &= (h11, h12, h13, h14, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0)\\
G1 &= (h21, h22, h23, h24, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0)\\
G2 &= (h31, h32, h33, h34, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0)\\
G3 &= (h11, h12, h13, h14, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0)\\
G4 &= (h21, h22, h23, h24, h11, h12, h13, h14, 0, 0, 0, 0, 0, 0, 0, 0)\\
G5 &= (h01, h02, h03, h04, h21, h22, h23, h24, 0, 0, 0, 0, 0, 0, 0, 0)\\
G6 &= (h01, h02, h03, h04, h21, h22, h23, h24, 0, 0, 0, 0, 0, 0, 0, 0)\\
G7 &= (h21, h22, h23, h24, h11, h12, h13, h14, 0, 0, 0, 0, 0, 0, 0, 0)\\
G8 &= (h11, h12, h13, h14, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0)\\
G9 &= (h31, h32, h33, h34, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0)
\end{aligned}$$

It is to be noted that a vector HH with constants in the above equations used as elements is the same as the vector HH of the first embodiment implementing the encryption level indicator calculation process as described earlier.

Next, a vector ZZ with its elements composing the right half of a sequence of initial values of the key-scheduling part is defined as follows.

[formula 26]

$$ZZ=(z31, z32, z33, z34, z35, z36, z37, z38, z41, z42, z43, z44, z45, z46, z47, z48)$$

By using these, the right half of the key-scheduling part in the Hierocrypt-3 common-key encryption algorithm is expressed below. It is to be noted that the operator + used in the following expressions is an additive operator in the Galois field GF(2).

[formula 27]

$Z0M5*ZZ+G0$

$W0=P32*Z0$

$Z1=M5*W0+G1$

$W1=P32*Z1$

$Z2=M5*W1+G2$

$W2=P32*Z2$

$Z3=M5*W2+G3$

$W3=P32*Z3$

$Z4=M5*W3+G4$

$W4=P32*Z4$

$Z5=M5*W4+G5$

$W6=MB*(Z5+G6)$

$Z6=P32I*W6$

$W7=MB*(Z6+G7)$

$Z7=P32I*W7$

$W8=MB*(Z7+G8)$

$Z8=P32I*W8$

$W9=MB*(Z8+G9)$

$Z9=P32I*W9$

Symbols Z0, Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, W0, W1, W2, W3, W5, W6, W7, W8 and W9 used in the above equations form the right half of the sequence of intermediate values of the key-scheduling part.

Next, these intermediate values are expressed by being split in accordance with the following equations.

[formula 28]

$$Zn=Zn_3||ZN_4$$
$$Wn=Wn_1||WN_2$$

Symbol || used in the above equations denotes a concatenation of vectors.

Next, let non-linear transformation part outputs of rounds be V0, V1, V2, V3, V4, V5, V6, V7, V8 and V9. Each of the outputs is a vector consisting of eight elements as follows.

[formula 29]

$$V0=(v01, v02, v03, v04, v05, v06, v07, v08)$$
$$V1=(v11, v12, v13, v14, v15, v16, v17, v18)$$
$$V2=(v21, v22, v23, v24, v25, v26, v27, v28)$$
$$V3=(v31, v32, v33, v34, v35, v36, v37, v38)$$
$$V4=(v41, v42, v43, v44, v45, v46, v47, v48)$$
$$V5=(v51, v52, v53, v54, v55, v56, v57, v58)$$
$$V6=(v61, v62, v63, v64, v65, v66, v67, v68)$$
$$V7=(v71, v72, v73, v74, v75, v76, v77, v78)$$
$$V8=(v81, v82, v83, v84, v85, v86, v87, v88)$$
$$V9=(v91, v92, v93, v94, v95, v96, v97, v98)$$

Here, vectors Z_1 and Z_2 are set as follows.

[formula 30]

$$Z_1=(z11, z12, z13, z14, z15, z16, z17, z18)$$
$$Z_2=(z21, z22, z23, z24, z25, z26, z27, z28)$$

With the vectors Z_1 and Z_2 set as described above, the left half of the sequence of the key-scheduling part in the Hierocrypt-3 common-key encryption algorithm is expressed as follows.

[formula 31]

$$Z0_1=Z_2$$
$$Z0_2=Z_1+V0$$
$$Z1_1=Z0_2$$
$$Z1_2=Z0_1+V1$$
$$Z2_1=Z1_2$$
$$Z2_2=Z1_1+V2$$
$$Z3_1=Z2_2$$
$$Z3_2=Z2_1+V3$$
$$Z4_1=Z3_2$$
$$Z4_2=Z3_1+V4$$
$$Z5_1=Z4_2$$
$$Z5_2=Z4_1+V5$$
$$Z6_1=Z5_2+V6$$
$$Z6_2=Z5_1$$
$$Z7_1=Z6_2+V7$$
$$Z7_2=Z6_1$$
$$Z8_1=Z7_2+V8$$
$$Z8_2=Z7_1$$
$$Z9_1=Z8_2+V9$$
$$Z9_2=Z8_1$$

Symbols $Z0_1$, $Z0_2$, $Z1_1$, $Z1_2$, $Z2_1$, $Z2_2$, $Z3_1$, $Z3_2$, $Z4_1$, $Z4_2$, $Z5_1$, $Z5_2$, $Z6_1$, $Z6_2$, $Z7_1$, $Z7_2$, $Z8_1$, $Z8_2$, $Z9_1$ and $Z9_2$ used in the above equations form the left half of the sequence of intermediate values of the key-scheduling part. By using the intermediate values obtained as described above, round keys $K1_1$, $K1_2$, $K1_3$, $K1_4$, $K2_1$, $\cdots$, $K9_1$ and $K9_2$ are expressed as follows:

[formula 32]

$K1_1 = Z0_1 + V1$

$K1_2 = Z1_3 + V1$

$K1_3 = Z1_4 + V1$

$K1_4 = Z0_2 + Z1_4$

$K2_1 = Z1_1 + V2$

$K2_2 = Z2_3 + V2$

$K2_3 = Z2_4 + V2$

$K2_4 = Z1_2 + Z2_4$

$K3_1 = Z2_1 + V3$

$K3_2 = Z3_3 + V3$

$K3_3 = Z3_4 + V3$

$K3_4 = Z2_2 + Z3_4$

$K4_1 = Z3_1 + V4$

$K4_2 = Z4_3 + V4$

$K4_3 = Z4_4 + V4$

$K4_4 = Z3_2 + Z4_4$

$K5_1 = Z4_1 + V5$

$K5_2 = Z5_3 + V5$

$K5_3 = Z5_4 + V5$

$K5_4 = Z4_2 + Z5_4$

$K6_1 = Z6_1 + Z5_3$

$K6_2 = W6_1 + V6$

$K6_3 = W6_2 + V6$

$K6_4 = Z5_1 + W6_2$

$K7_1=Z7_1+Z6_3$

$K7_2=W7_1+V7$

$K7_3=W7_2+V7$

$K7_4=Z6_1+W7_2$

$K8_1=Z8_1+Z7_3$

$K8_2=W8_1+V8$

$K8_3=W8_2+V8$

$K8_4=Z7_1+W8_2$

$K9_1=Z9_1+Z8_3$

$K9_2=W9_1+V9$

$K9_3=W9_2+V9$

$K9_4=Z8_1+W9_2$

It is to be noted that symbols K11, K12, K13, K14, K21, ···, K91 and K92 each denote a vector consisting of eight elements.

The following description explains the step S102 of carrying out a process to eliminate intermediate variables in the processing represented by the flowchart shown in Fig. 1. If the eight elements of each of the vectors K11, K12, K13, K14, K21, ···, K91 and K92 are expressed by their actual values, the vectors K11, K12, K13, K14, K21, ···, K91 and K92 can be expressed as follows:

[formula 33]

$$
K1_1 = \begin{pmatrix}
v11 + z21 \\
v12 + z22 \\
v13 + z23 \\
v14 + z24 \\
v15 + z25 \\
v16 + z26 \\
v17 + z27 \\
v18 + z28
\end{pmatrix}
$$

$$
K1_2 = \begin{pmatrix}
h11 + h21 + h13 + v11 + z32 + z42 \\
h11 + h12 + h22 + h14 + v12 + z33 + z43 \\
h11 + h12 + h13 + h23 + v13 + z31 + z41 + z34 + z44 \\
h12 + h14 + h24 + v14 + z31 + z41 \\
h01 + h02 + h03 + h04 + h31 + v15 + z36 + z46 + z38 + z48 \\
h02 + h03 + h04 + h32 + v16 + z35 + z45 + z37 + z47 \\
h03 + h04 + h33 + v17 + z35 + z36 + z45 + z46 + z38 + z48 \\
h01 + h02 + h03 + h34 + v18 + z35 + z45 + z37 + z38 + z47 + z48
\end{pmatrix}
$$

$$K1_3 = \begin{pmatrix} h01 + h03 + v11 + z42 + z35 + z36 + z45 + z46 \\ h01 + h02 + h04 + v12 + z43 + z36 + z37 + z46 + z47 \\ h01 + h02 + h03 + v13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48 \\ h02 + h04 + v14 + z41 + z35 + z45 + z38 + z43 \\ h11 + h12 + h13 + h14 + v15 + z31 + z32 + z41 + z42 + z46 + z48 \\ h12 + h13 + h14 + v16 + z32 + z33 + z42 + z43 + z45 + z47 \\ h13 + h14 + v17 + z31 + z41 + z33 + z34 + z43 + z44 + z45 + z46 + z48 \\ h11 + h12 + h13 + z31 + v18 + z41 + z34 + z44 + z45 + z47 + z48 \end{pmatrix}$$

$$K1_4 = \begin{pmatrix} h01 + h03 + v01 + z11 + z42 + z35 + z36 + z45 + z46 \\ h01 + h02 + h04 + v02 + z12 + z43 + z36 + z37 + z46 + z47 \\ h01 + h02 + h03 + v03 + z13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48 \\ h02 + h04 + v04 + z14 + z41 + z35 + z45 + z38 + z48 \\ h11 + h12 + h13 + h14 + v05 + z31 + z32 + z41 + z15 + z42 + z46 + z48 \\ h12 + h13 + h14 + v06 + z32 + z33 + z42 + z16 + z43 + z45 + z47 \\ h13 + h14 + v07 + z31 + z41 + z33 + z34 + z43 + z17 + z44 + z45 + z46 + z48 \\ h11 + h12 + h13 + v08 + z31 + z41 + z34 + z44 + z18 + z45 + z47 + z48 \end{pmatrix}$$

$$K2_1 = \begin{pmatrix} v01 + v21 + z11 \\ v02 + v22 + z12 \\ v03 + v23 + z13 \\ v04 + v24 + z14 \\ v05 + v25 + z15 \\ v06 + v26 + z16 \\ v07 + v27 + z17 \\ v08 + v28 + z18 \end{pmatrix}$$

$$K2_2 = \begin{pmatrix} h02 + h12 + h21 + h31 + h23 + v21 + z31 + z32 + z34 + z36 + z37 + z46 + z38 \\ +z47 + z48 \\ h03 + h21 + h13 + h22 + h32 + h24 + v22 + z31 + z32 + z33 + z37 + z38 + z47 \\ +z48 \\ h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + v23 + z31 + z32 + z33 + z34 \\ +z38 + z48 \\ h01 + h11 + h22 + h24 + h34 + v24 + z31 + z33 + z35 + z36 + z45 + z37 + z46 \\ +z38 + z47 + z48 \\ h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + v25 + z31 + z41 + z35 \\ +z38 \\ h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + v26 + z32 + z42 + z35 + z36 \\ h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + v27 + z33 + z43 + z36 \\ +z37 \\ h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + v28 + z34 + z44 + z37 \end{pmatrix}$$

$$K2_3 = \begin{pmatrix} h01 + h11 + h12 + h31 + h33 + v21 + z32 + z41 + z33 + z34 + z43 + z35 + z36 \\ + z37 + z46 + z38 + z47 + z48 \\ h02 + h12 + h13 + h31 + h32 + h34 + v22 + z41 + z33 + z42 + z34 + z44 + z36 \\ + z37 + z38 + z47 + z48 \\ h11 + h03 + h13 + h31 + h14 + h32 + h33 + v23 + z41 + z42 + z34 + z43 + z37 \\ + z38 + z48 \\ h11 + h04 + h14 + h32 + h34 + v24 + z31 + z32 + z33 + z42 + z34 + z35 + z44 \\ + z36 + z45 + z37 + z46 + z47 + z48 \\ h01 + h02 + h11 + h21 + h22 + h14 + h23 + h24 + v25 + z31 + z32 + z41 + z33 \\ + z34 + z35 + z48 \\ h02 + h11 + h03 + h12 + h22 + h23 + h24 + v26 + z32 + z33 + z42 + z34 + z36 \\ + z45 \\ h01 + h03 + h12 + h04 + h13 + h23 + h24 + v27 + z33 + z34 + z43 + z37 + z46 \\ h01 + h21 + h04 + h13 + h22 + h23 + z31 + z32 + v28 + z33 + z44 + z38 + z47 \\ + z48 \end{pmatrix}$$

$$K2_4 = \begin{pmatrix} h01 + h11 + h12 + h31 + h33 + v11 + z21 + z32 + z41 + z33 + z34 + z43 + z35 \\ + z36 + z37 + z46 + z38 + z47 + z48 \\ h02 + h12 + h13 + h31 + h32 + h34 + v12 + z22 + z41 + z33 + z42 + z34 + z44 \\ + z36 + z37 + z38 + z47 + z48 \\ h11 + h03 + h13 + h31 + h14 + h32 + h33 + v13 + z23 + z41 + z42 + z34 + z43 \\ + z37 + z38 + z48 \\ h11 + h04 + h14 + h32 + h34 + v14 + z31 + z32 + z24 + z33 + z42 + z34 + z35 \\ + z44 + z36 + z45 + z37 + z46 + z47 + z48 \\ h01 + h02 + h11 + h21 + h22 + h14 + h23 + h24 + v15 + z31 + z32 + z41 + z33 \\ + z25 + z34 + z35 + z48 \\ h02 + h11 + h03 + h12 + h22 + h23 + h24 + v16 + z32 + z33 + z42 + z34 + z26 \\ + z36 + z45 \\ h01 + h03 + h12 + h04 + h13 + h23 + h24 + v17 + z33 + z34 + z43 + z27 + z37 \\ + z46 \\ h01 + h21 + h04 + h13 + h22 + h23 + z31 + v18 + z32 + z33 + z44 + z28 + z38 \\ + z47 + z48 \end{pmatrix}$$

$$K3_1 = \begin{pmatrix} v11 + v31 + z21 \\ v12 + v32 + z22 \\ v13 + v33 + z23 \\ v14 + v34 + z24 \\ v15 + v35 + z25 \\ v16 + v36 + z26 \\ v17 + v37 + z27 \\ v18 + v38 + z28 \end{pmatrix}$$

$$K3_2 = \left(\begin{array}{l}
h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + v31 + z32 + z42 + z35 + z37 \\
h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + v32 + z33 + z43 + z35 \\
+z36 + z38 \\
h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + v33 + z31 + z41 + z34 + z35 \\
+z44 + z36 + z37 \\
h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + v34 + z31 + z41 + z36 \\
+z38 \\
h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + v35 + z31 + z33 + z35 \\
+z36 + z45 + z37 + z46 + z47 \\
h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + z31 + v36 + z32 \\
+z34 + z35 + z36 + z45 + z37 + z46 + z38 + z47 + z48 \\
h02 + h03 + h21 + h04 + h13 + h22 + h31 + h32 + h24 + h33 + h34 + z31 + z32 \\
+v37 + z33 + z36 + z37 + z46 + z38 + z47 + z48 \\
h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + z32 + v38 + z34 + z35 \\
+z36 + z45 + z46 + z38 + z48
\end{array}\right)$$

$$K3_3 = \left(\begin{array}{l}
h01 + h02 + h03 + h21 + h04 + h22 + h31 + v31 + z42 + z35 + z38 + z47 + z48 \\
h02 + h03 + h04 + h22 + h23 + h32 + v32 + z43 + z35 + z36 + z48 \\
h03 + h21 + h04 + h23 + h24 + h33 + v33 + z41 + z44 + z36 + z45 + z37 \\
h01 + h02 + h03 + h21 + h24 + h34 + v34 + z41 + z37 + z46 + z47 + z48 \\
h11 + h12 + h21 + h13 + h24 + h33 + h34 + v35 + z31 + z34 + z43 + z44 + z45 \\
+z46 + z47 \\
h11 + h12 + h21 + h13 + h22 + h14 + h34 + z31 + v36 + z32 + z44 + z45 + z46 \\
+z47 + z48 \\
h12 + h13 + h22 + h31 + h14 + h23 + z32 + z41 + v37 + z33 + z46 + z47 + z48 \\
h11 + h12 + h14 + h23 + h32 + h33 + h34 + z33 + z42 + v38 + z43 + z44 + z45 \\
+z46 + z48
\end{array}\right)$$

$$K3_4 = \begin{pmatrix} h01 + h02 + h03 + h21 + h04 + h22 + h31 + v01 + v21 + z11 + z42 + z35 + z38 \\ +z47 + z48 \\ h02 + h03 + h04 + h22 + h23 + h32 + v02 + v22 + z12 + z43 + z35 + z36 + z48 \\ h03 + h21 + h04 + h23 + h24 + h33 + v03 + v23 + z13 + z41 + z44 + z36 + z45 \\ +z37 \\ h01 + h02 + h03 + h21 + h24 + h34 + v04 + v24 + z14 + z41 + z37 + z46 + z47 \\ +z48 \\ h11 + h12 + h21 + h13 + h24 + h33 + h34 + v05 + v25 + z31 + z15 + z34 + z43 \\ +z44 + z45 + z46 + z47 \\ h11 + h12 + h21 + h13 + h22 + h14 + h34 + v06 + v26 + z31 + z32 + z16 + z44 \\ +z45 + z46 + z47 + z48 \\ h12 + h13 + h22 + h31 + h14 + h23 + v07 + v27 + z32 + z41 + z33 + z17 + z46 \\ +z47 + z48 \\ h11 + h12 + h14 + h23 + h32 + h33 + h34 + v08 + v28 + z33 + z42 + z43 + z44 \\ +z18 + z45 + z46 + z48 \end{pmatrix}$$

$$K4_1 = \begin{pmatrix} v01 + v21 + v41 + z11 \\ v02 + v22 + v42 + z12 \\ v03 + v23 + v43 + z13 \\ v04 + v24 + v44 + z14 \\ v05 + v25 + v45 + z15 \\ v06 + v26 + v46 + z16 \\ v07 + v27 + v47 + z17 \\ v08 + v28 + v48 + z18 \end{pmatrix}$$

$$K4_2 = \begin{pmatrix} h01 + h11 + h03 + h12 + h13 + h23 + h33 + h34 + v41 + z31 + z32 + z34 + z35 + z45 \\ +z37 + z38 + z47 + z48 \\ h01 + h02 + h11 + h12 + h21 + h04 + h13 + h14 + h24 + h34 + v42 + z31 + z32 + z33 \\ +z36 + z46 + z38 + z48 \\ h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h14 + v43 + z31 + z32 + z33 + z34 \\ +z35 + z45 + z37 + z47 \\ h02 + h11 + h12 + h04 + h22 + h14 + h32 + h33 + h34 + v44 + z31 + z33 + z36 + z37 \\ +z46 + z47 \\ h01 + h11 + h03 + h12 + h21 + h04 + h31 + h33 + h34 + z31 + v45 + z32 + z41 + z42 \\ +z34 + z35 + z44 + z37 + z38 \\ h02 + h12 + h04 + h13 + h22 + h32 + h34 + z31 + z32 + z41 + v46 + z33 + z42 + z43 \\ +z36 + z38 \\ h01 + h11 + h03 + h13 + h31 + h14 + h23 + h33 + z31 + z32 + z41 + z33 + z42 + v47 \\ +z34 + z43 + z35 + z44 + z37 \\ h02 + h11 + h03 + h14 + h32 + h24 + h33 + z31 + z41 + z33 + z43 + v48 + z36 + z37 \end{pmatrix}$$

$$K4_3 = \begin{pmatrix} h02+h04+h13+h14+h33+h34+v41+z31+z33+z42+z34+z43+z36+z45 \\ +z37+z47+z48 \\ h01+h03+h14+h34+v42+z32+z41+z34+z43+z35+z44+z37+z46+z38 \\ +z48 \\ h01+h02+h11+h04+h31+v43+z31+z33+z42+z44+z36+z45+z38+z47 \\ h01+h03+h12+h04+h13+h14+h32+h33+h34+v44+z32+z41+z33+z42 \\ +z35+z36+z46+z47 \\ h01+h02+h11+h03+h21+h04+h22+h31+h23+h34+v45+z32+z41+z33 \\ +z42+z35+z44+z36+z46+z38+z47 \\ h02+h03+h12+h21+h04+h22+h31+h23+h32+h24+z31+z41+v46+z33 \\ +z42+z34+z43+z35+z36+z45+z37+z47+z48 \\ h03+h04+h13+h22+h23+h32+h24+h33+z32+z41+z42+v47+z34+z43 \\ +z35+z44+z36+z37+z46+z38+z48 \\ h01+h02+h03+h21+h22+h14+h24+h33+z31+z32+z41+z43+v48+z35 \\ +z45+z37+z46 \end{pmatrix}$$

$$K4_4 = \begin{pmatrix} h02+h04+h13+h14+h33+h34+v11+v31+z21+z31+z33+z42+z34+z43 \\ +z36+z45+z37+z47+z48 \\ h01+h03+h14+h34+v12+v32+z22+z32+z41+z34+z43+z35+z44+z37 \\ +z46+z38+z48 \\ h01+h02+h11+h04+h31+v13+v33+z31+z23+z33+z42+z44+z36+z45 \\ +z38+z47 \\ h01+h03+h12+h04+h13+h14+h32+h33+h34+v14+v34+z32+z41+z24 \\ +z33+z42+z35+z36+z46+z47 \\ h01+h02+h11+h03+h21+h04+h22+h31+h23+h34+v15+v35+z32+z41 \\ +z33+z42+z25+z35+z44+z36+z46+z38+z47 \\ h02+h03+h12+h21+h04+h22+h31+h23+h32+h24+v16+z31+v36+z41 \\ +z33+z42+z34+z43+z26+z35+z36+z45+z37+z47+z48 \\ h03+h04+h13+h22+h23+h32+h24+h33+v17+z32+z41+v37+z42+z34 \\ +z43+z35+z44+z27+z36+z37+z46+z38+z48 \\ h01+h02+h03+h21+h22+h14+h24+h33+z31+v18+z32+z41+v38+z43 \\ +z35+z45+z28+z37+z46 \end{pmatrix}$$

$$K5_1 = \begin{pmatrix} v11+v31+v51+z21 \\ v12+v32+v52+z22 \\ v13+v33+v53+z23 \\ v14+v34+v54+z24 \\ v15+v35+v55+z25 \\ v16+v36+v56+z26 \\ v17+v37+v57+z27 \\ v18+v38+v58+z28 \end{pmatrix}$$

$$K5_2 = \begin{pmatrix} h02 + h21 + h13 + h22 + h23 + v51 + z33 + z34 + z43 + z44 + z37 \\ h11 + h03 + h21 + h22 + h14 + h23 + h24 + v52 + z34 + z35 + z44 + z38 \\ h01 + h11 + h12 + h04 + h22 + h23 + h24 + v53 + z31 + z41 + z35 + z36 \\ h01 + h12 + h21 + h22 + h24 + v54 + z32 + z33 + z42 + z34 + z43 + z44 + z36 \\ h02 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + v55 + z33 + z36 + z46 \\ h03 + h04 + h13 + h22 + h14 + h23 + h34 + z31 + v56 + z34 + z37 + z47 \\ h21 + h04 + h31 + h14 + h23 + h24 + z31 + z32 + v57 + z35 + z45 + z38 + z48 \\ h01 + h02 + h11 + h03 + h12 + h21 + h04 + h13 + h14 + h32 + h24 + h33 + h34 + z32 \\ + z35 + v58 + z45 \end{pmatrix}$$

$$K5_3 = \begin{pmatrix} h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + v51 + z43 + z44 + z47 \\ h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + v52 + z44 + z45 + z48 \\ h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + v53 + z41 + z45 + z46 \\ h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + v54 + z42 + z43 \\ + z44 + z46 \\ h11 + h21 + h14 + h34 + v55 + z43 + z46 \\ h11 + h12 + h22 + h31 + z41 + v56 + z44 + z47 \\ h12 + h13 + h23 + h32 + z41 + z42 + v57 + z45 + z48 \\ h13 + h24 + h33 + h34 + z42 + v58 + z45 \end{pmatrix}$$

$$K5_4 = \begin{pmatrix} h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + v01 + v21 + v41 + z11 + z43 \\ + z44 + z47 \\ h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + v02 + v22 + v42 + z12 + z44 \\ + z45 + z48 \\ h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + v03 + v23 + v43 + z13 \\ + z41 + z45 + z46 \\ h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + v04 + v24 \\ + v44 + z14 + z42 + z43 + z44 + z46 \\ h11 + h21 + h14 + h34 + v05 + v25 + v45 + z15 + z43 + z46 \\ h11 + h12 + h22 + h31 + v06 + v26 + z41 + v46 + z16 + z44 + z47 \\ h12 + h13 + h23 + h32 + v07 + v27 + z41 + z42 + v47 + z17 + z45 + z48 \\ h13 + h24 + h33 + h34 + v08 + v28 + z42 + v48 + z18 + z45 \end{pmatrix}$$

$$K6_1 = \left(\begin{array}{l}
h02 + h21 + h13 + h22 + h23 + v11 + v31 + v51 + v61 + z21 + z33 + z34 + z43 \\
+z44 + z37 \\
h11 + h03 + h21 + h22 + h14 + h23 + h24 + v12 + v32 + v52 + v62 + z22 + z34 \\
+z35 + z44 + z38 \\
h01 + h11 + h12 + h04 + h22 + h23 + h24 + v13 + v33 + v53 + z31 + v63 + z23 \\
+z41 + z35 + z36 \\
h01 + h12 + h21 + h22 + h24 + v14 + v34 + v54 + z32 + v64 + z24 + z33 + z42 \\
+z34 + z43 + z44 + z36 \\
h02 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + v15 + v35 + v55 \\
+z33 + v65 + z25 + z36 + z46 \\
h03 + h04 + h13 + h22 + h14 + h23 + h34 + v16 + z31 + v36 + v56 + z34 + v66 \\
+z26 + z37 + z47 \\
h21 + h04 + h31 + h14 + h23 + h24 + v17 + z31 + z32 + v37 + v57 + z35 + v67 \\
+z27 + z45 + z38 + z48 \\
h01 + h02 + h11 + h03 + h12 + h21 + h04 + h13 + h14 + h32 + h24 + h33 + h34 \\
+v18 + z32 + v38 + z35 + v58 + z45 + v68 + z28
\end{array}\right)$$

$$K6_2 = \left(\begin{array}{l}
h01 + h02 + h11 + h03 + h12 + h04 + h14 + h23 + v61 + z32 + z33 + z42 + z43 \\
+z35 + z36 + z38 \\
h02 + h11 + h03 + h12 + h21 + h04 + h13 + h24 + v62 + z31 + z41 + z33 + z34 \\
+z43 + z35 + z44 + z36 + z37 \\
h11 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + v63 + z32 + z42 + z34 + z35 \\
+z44 + z36 + z37 + z38 \\
h01 + h02 + h11 + h03 + h13 + h22 + z31 + z32 + z41 + v64 + z42 + z35 + z37 \\
h02 + h12 + h22 + h23 + h33 + z31 + z33 + v65 + z34 + z36 + z37 + z46 + z47 \\
h03 + h21 + h13 + h31 + h23 + h24 + h34 + z32 + z34 + v66 + z35 + z45 + z37 \\
+z38 + z47 + z48 \\
h01 + h11 + h04 + h22 + h31 + h14 + h32 + h24 + z31 + z33 + v67 + z36 + z46 \\
+z38 + z48 \\
h01 + h11 + h21 + h22 + h32 + z32 + z33 + z35 + z36 + z45 + v68 + z46
\end{array}\right)$$

$$K6_3 = \left(\begin{array}{l}
h12 + h04 + h13 + h22 + h14 + h23 + h34 + v61 + z42 + z43 + z45 + z46 + z48 \\
h01 + h21 + h13 + h31 + h14 + h23 + h24 + v62 + z41 + z43 + z44 + z45 + z46 \\
+z47 \\
h02 + h22 + h14 + h32 + h24 + v63 + z42 + z44 + z45 + z46 + z47 + z48 \\
h11 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + z41 + v64 + z42 \\
+z45 + z47 \\
h12 + h21 + h22 + h31 + h14 + h34 + z41 + v65 + z43 + z44 + z46 + z47 \\
h11 + h13 + h22 + h31 + h23 + h32 + z42 + v66 + z44 + z45 + z47 + z48 \\
h11 + h12 + h21 + h14 + h23 + h32 + h24 + h33 + z41 + z43 + v67 + z46 + z48 \\
h11 + h21 + h13 + h14 + h24 + h33 + z42 + z43 + z45 + v68 + z46
\end{array}\right)$$

$$K6_4 = \left(\begin{array}{l} h12 + h04 + h13 + h22 + h14 + h23 + h34 + v01 + v21 + v41 + z11 + z42 + z43 \\ + z45 + z46 + z48 \\ h01 + h21 + h13 + h31 + h14 + h23 + h24 + v02 + v22 + v42 + z12 + z41 + z43 \\ + z44 + z45 + z46 + z47 \\ h02 + h22 + h14 + h32 + h24 + v03 + v23 + v43 + z13 + z42 + z44 + z45 + z46 \\ + z47 + z48 \\ h11 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + v04 + v24 + v44 \\ + z14 + z41 + z42 + z45 + z47 \\ h12 + h21 + h22 + h31 + h14 + h34 + v05 + v25 + v45 + z41 + z15 + z43 + z44 \\ + z46 + z47 \\ h11 + h13 + h22 + h31 + h23 + h32 + v06 + v26 + v46 + z42 + z16 + z44 + z45 \\ + z47 + z48 \\ h11 + h12 + h21 + h14 + h23 + h32 + h24 + h33 + v07 + v27 + z41 + v47 + z43 \\ + z17 + z46 + z48 \\ h11 + h21 + h13 + h14 + h24 + h33 + v08 + v28 + z42 + z43 + v48 + z18 + z45 \\ + z46 \end{array} \right)$$

$$K7_1 = \left(\begin{array}{l} h01 + h11 + h03 + h12 + h13 + h23 + h33 + h34 + v01 + v21 + v41 + z11 + v71 \\ + z31 + z32 + z34 + z35 + z45 + z37 + z38 + z47 + z48 \\ h01 + h02 + h11 + h12 + h21 + h04 + h13 + h14 + h24 + h34 + v02 + v22 + v42 \\ + z12 + z31 + v72 + z32 + z33 + z36 + z46 + z38 + z48 \\ h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h14 + v03 + v23 + v43 + z13 \\ + z31 + z32 + v73 + z33 + z34 + z35 + z45 + z37 + z47 \\ h02 + h11 + h12 + h04 + h22 + h14 + h32 + h33 + h34 + v04 + v24 + v44 + z31 \\ + z14 + z33 + v74 + z36 + z37 + z46 + z47 \\ h01 + h11 + h03 + h12 + h21 + h04 + h31 + h33 + h34 + v05 + v25 + z31 + v45 \\ + z32 + z41 + z15 + z42 + z34 + v75 + z35 + z44 + z37 + z38 \\ h02 + h12 + h04 + h13 + h22 + h32 + h34 + v06 + v26 + z31 + z32 + z41 + v46 \\ + z33 + z42 + z16 + z43 + v76 + z36 + z38 \\ h01 + h11 + h03 + h13 + h31 + h14 + h23 + h33 + v07 + z31 + v27 + z32 + z41 \\ + z33 + z42 + v47 + z34 + z43 + z17 + z35 + z44 + v77 + z37 \\ h02 + h11 + h03 + h14 + h32 + h24 + h33 + v08 + z31 + z41 + v28 + z33 + z43 \\ + v48 + z18 + z36 + z37 + v78 \end{array} \right)$$

$$
K7_2 = \begin{pmatrix}
h01 + h21 + h13 + h32 + h33 + v71 + z32 + z37 + z38 + z47 + z48 \\
h02 + h11 + h22 + h31 + h14 + h33 + h34 + v72 + z33 + z38 + z48 \\
h11 + h03 + h12 + h23 + h32 + h34 + z31 + v73 + z34 + z35 + z45 \\
h12 + h04 + h31 + h32 + h24 + z31 + v74 + z36 + z37 + z46 + z38 + z47 + z48 \\
h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h32 + h33 + z33 + z34 + z43 \\
+v75 + z35 + z44 + z36 + z37 \\
h01 + h02 + h11 + h03 + h04 + h13 + h22 + h31 + h14 + h23 + h32 + h33 + h34 \\
+z34 + z35 + z44 + v76 + z36 + z37 + z38 \\
h02 + h03 + h12 + h21 + h04 + h14 + h23 + h32 + h24 + h33 + h34 + z31 + z41 \\
+z36 + v77 + z37 + z38 \\
h01 + h02 + h11 + h12 + h21 + h04 + h31 + h32 + h24 + h34 + z32 + z33 + z42 \\
+z34 + z43 + z35 + z44 + z36 + v78 + z38
\end{pmatrix}
$$

$$
K7_3 = \begin{pmatrix}
h12 + h04 + h13 + h32 + h33 + v71 + z33 + z42 + z34 + z43 + z44 + z36 + z37 \\
+z38 + z47 + z48 \\
h01 + h11 + h13 + h31 + h14 + h33 + h34 + v72 + z34 + z43 + z44 + z37 + z38 + z48 \\
h02 + h12 + h14 + h32 + h34 + z31 + v73 + z44 + z45 + z38 \\
h11 + h03 + h12 + h04 + h31 + h32 + z32 + z41 + z33 + z42 + v74 + z34 + z43 \\
+z35 + z44 + z36 + z37 + z46 + z38 + z47 + z48 \\
h01 + h11 + h12 + h32 + h24 + h34 + z31 + z32 + z34 + z43 + v75 + z44 + z45 \\
+z37 + z46 + z38 + z48 \\
h02 + h12 + h21 + h13 + h31 + h33 + z31 + z32 + z33 + z44 + v76 + z45 + z46 \\
+z38 + z47 \\
h11 + h03 + h13 + h22 + h31 + h14 + h32 + h34 + z31 + z32 + z41 + z33 + z34 \\
+z35 + z45 + v77 + z46 + z47 + z48 \\
h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + z33 + z42 + z43 + z44 \\
+z36 + z45 + z37 + v78 + z38 + z47
\end{pmatrix}
$$

$$K7_4 = \begin{pmatrix} h12 + h04 + h13 + h32 + h33 + v11 + v31 + v51 + v61 + z21 + z33 + z42 + z34 + z43 \\ +z44 + z36 + z37 + z38 + z47 + z48 \\ h01 + h11 + h13 + h31 + h14 + h33 + h34 + v12 + v32 + v52 + v62 + z22 + z34 + z43 \\ +z44 + z37 + z38 + z48 \\ h02 + h12 + h14 + h32 + h34 + v13 + v33 + v53 + z31 + v63 + z23 + z44 + z45 + z38 \\ h11 + h03 + h12 + h04 + h31 + h32 + v14 + v34 + v54 + z32 + z41 + v64 + z24 + z33 \\ +z42 + z34 + z43 + z35 + z44 + z36 + z37 + z46 + z38 + z47 + z48 \\ h01 + h11 + h12 + h32 + h24 + h34 + v15 + v35 + z31 + z32 + v55 + v65 + z25 + z34 \\ +z43 + z44 + z45 + z37 + z46 + z38 + z48 \\ h02 + h12 + h21 + h13 + h31 + h33 + v16 + z31 + v36 + z32 + z33 + v56 + v66 + z26 \\ +z44 + z45 + z46 + z38 + z47 \\ h11 + h03 + h13 + h22 + h31 + h14 + h32 + h34 + v17 + z31 + z32 + z41 + v37 + z33 \\ +z34 + v57 + z35 + v67 + x27 + z45 + z46 + z47 + z48 \\ h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + v18 + z33 + z42 + v38 + z43 \\ +z44 + v58 + z36 + z45 + v68 + z28 + z37 + z38 + z47 \end{pmatrix}$$

$$K8_1 = \begin{pmatrix} h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + v11 + v31 + v51 + v61 + z21 + v81 \\ +z32 + z42 + z35 + z37 \\ h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + v12 + v32 + v52 + v62 + z22 \\ +v82 + z33 + z43 + z35 + z36 + z38 \\ h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + v13 + v33 + v53 + z31 + v63 + z23 \\ +z41 + v83 + z34 + z35 + z44 + z36 + z37 \\ h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + v14 + v34 + z31 + v54 + z41 \\ +v64 + z24 + v84 + z36 + z38 \\ h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + v15 + v35 + z31 + v55 + z33 \\ +v65 + z25 + z35 + v85 + z36 + z45 + z37 + z46 + z47 \\ h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + v16 + z31 + v36 + z32 \\ +v56 + z34 + v66 + z26 + z35 + z36 + z45 + v86 + z37 + z46 + z38 + z47 + z48 \\ h02 + h03 + h21 + h04 + h13 + h22 + h31 + h32 + h24 + h33 + h34 + v17 + z31 + z32 \\ +v37 + z33 + v57 + v67 + z27 + z36 + z37 + z46 + v87 + z38 + z47 + z48 \\ h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + v18 + z32 + v38 + z34 + z35 \\ +v58 + z36 + z45 + v68 + z28 + z46 + z38 + v88 + z48 \end{pmatrix}$$

$$K8_2 = \left(\begin{array}{l}
h01 + h02 + h11 + h21 + h23 + h33 + z31 + v81 + z41 + z33 + z43 + z35 \\
h02 + h03 + h12 + h21 + h22 + h31 + h24 + h34 + z31 + z32 + z41 + v82 + z42 + z34 \\
+ z44 + z36 \\
h01 + h03 + h21 + h04 + h13 + h22 + h31 + h23 + h32 + z31 + z32 + z41 + z33 + z42 \\
+ v83 + z43 + z37 \\
h01 + h04 + h22 + h14 + h32 + h24 + z32 + z42 + z34 + v84 + z44 + z38 \\
h11 + h12 + h21 + h04 + h22 + h31 + h23 + h32 + h24 + h33 + h34 + z32 + z33 + z34 \\
+ v85 + z38 + z48 \\
h01 + h12 + h13 + h22 + h23 + h32 + h24 + h33 + h34 + z33 + z34 + z35 + z45 + v86 \\
h02 + h11 + h13 + h14 + h23 + h24 + h33 + h34 + z34 + z36 + z46 + v87 \\
h11 + h03 + h21 + h04 + h22 + h31 + h14 + h23 + h32 + h33 + z31 + z32 + z33 + z34 \\
+ z37 + z38 + z47 + v88 + z48
\end{array}\right)$$

$$K8_3 = \left(\begin{array}{l}
h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + v81 + z41 + z43 + z35 + z36 \\
+ z37 + z46 + z47 \\
h01 + h02 + h22 + h31 + h23 + h24 + h33 + z41 + v82 + z42 + z35 + z44 + z36 \\
+ z45 + z37 + z38 + z47 + z48 \\
h02 + h03 + h31 + h23 + h32 + h24 + h34 + z41 + z42 + v83 + z43 + z36 + z37 \\
+ z46 + z38 + z48 \\
h03 + h21 + h22 + h31 + h23 + h33 + h34 + z42 + v84 + z35 + z44 + z36 + z45 \\
+ z46 + z38 \\
h22 + h14 + h24 + h33 + z32 + z34 + z43 + v85 + z48 \\
h11 + h21 + h31 + h23 + h34 + z31 + z41 + z33 + z44 + z45 + v86 \\
h12 + h21 + h22 + h31 + h32 + h24 + z31 + z32 + z41 + z42 + z34 + z46 + v87 \\
h21 + h13 + h14 + h23 + h32 + h24 + z31 + z33 + z42 + z34 + z47 + v88 + z48
\end{array}\right)$$

$$K8_4 = \left(\begin{array}{l}
h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + v01 + v21 + v41 + z11 + v71 \\
+ z41 + z43 + z35 + z36 + z37 + z46 + z47 \\
h01 + h02 + h22 + h31 + h23 + h24 + h33 + v02 + v22 + v42 + z12 + v72 + z41 \\
+ z42 + z35 + z44 + z36 + z45 + z37 + z38 + z47 + z48 \\
h02 + h03 + h31 + h23 + h32 + h24 + h34 + v03 + v23 + v43 + z13 + z41 + v73 \\
+ z42 + z43 + z36 + z37 + z46 + z38 + z48 \\
h03 + h21 + h22 + h31 + h23 + h33 + h34 + v04 + v24 + v44 + z14 + z42 + v74 \\
+ z35 + z44 + z36 + z45 + z46 + z38 \\
h22 + h14 + h24 + h33 + v05 + v25 + v45 + z32 + z15 + z34 + z43 + v75 + z48 \\
h11 + h21 + h31 + h23 + h34 + v06 + v26 + z31 + z41 + v46 + z33 + z16 + z44 \\
+ v76 + z45 \\
h12 + h21 + h22 + h31 + h32 + h24 + v07 + z31 + v27 + z32 + z41 + z42 + v47 \\
+ z34 + z17 + v77 + z46 \\
h21 + h13 + h14 + h23 + h32 + h24 + v08 + z31 + v28 + z33 + z42 + z34 + v48 \\
+ z18 + v78 + z47 + z48
\end{array}\right)$$

$$K9_1 = \left(\begin{array}{l}
h02 + h12 + h21 + h31 + h23 + v01 + v21 + v41 + z11 + v71 + z31 + z32 + v91 \\
+z34 + z36 + z37 + z46 + z38 + z47 + z48 \\
h03 + h21 + h13 + h22 + h32 + h24 + v02 + v22 + v42 + z12 + z31 + v72 + z32 \\
+z33 + v92 + z37 + z38 + z47 + z48 \\
h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + v03 + v23 + v43 + z13 + z31 \\
+z32 + v73 + z33 + z34 + v93 + z38 + z48 \\
h01 + h11 + h22 + h24 + h34 + v04 + v24 + v44 + z31 + z14 + z33 + v74 + z35 \\
+v94 + z36 + z45 + z37 + z46 + z38 + z47 + z48 \\
h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + v05 + v25 + z31 + v45 \\
+z41 + z15 + v75 + z35 + v95 + z38 \\
h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + v06 + v26 + z32 + v46 + z42 \\
+z16 + z35 + v76 + z36 + v96 \\
h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + v07 + v27 + z33 + v47 \\
+z43 + z17 + z36 + v77 + z37 + v97 \\
h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + v08 + v28 + z34 + v48 + z44 \\
+z18 + z37 + v78 + v98
\end{array}\right)$$

$$K9_2 = \left(\begin{array}{l}
h01 + h11 + h03 + h21 + h13 + z32 + v91 + z35 + z36 + z45 + z46 \\
h01 + h02 + h11 + h12 + h04 + h22 + h14 + z33 + v92 + z36 + z37 + z46 + z47 \\
h01 + h02 + h11 + h03 + h12 + h13 + h23 + z31 + z34 + v93 + z35 + z45 + z37 \\
+z38 + z47 + z48 \\
h02 + h12 + h04 + h14 + h24 + z31 + z35 + v94 + z45 + z38 + z48 \\
h01 + h02 + h11 + h03 + h12 + h04 + h13 + h31 + h14 + z31 + z32 + z41 + z42 \\
+z36 + v95 + z38 \\
h02 + h03 + h12 + h04 + h13 + h14 + h32 + z32 + z33 + z42 + z43 + z35 + z37 \\
+v96 \\
h03 + h04 + h13 + h14 + h33 + z31 + z41 + z33 + z34 + z43 + z35 + z44 + z36 \\
+z38 + v97 \\
h01 + h02 + h11 + h03 + h12 + h13 + h34 + z31 + z41 + z34 + z35 + z44 + z37 \\
+z38 + v98
\end{array}\right)$$

Then, the next step S103 is executed to carry out a variable transposition process. With the results of the vectors K11, K12, K13, K14, K21, ···, K91 and K92 used as a base, the simultaneous linear equation is transformed so as to result in equations, which each include only terms zxx and vxx on the right-hand side thereof as follows.

[formula 34]

$$k1_{11} = v11 + z21$$
$$k1_{12} = v12 + z22$$
$$k1_{13} = v13 + z23$$
$$k1_{14} = v14 + z24$$
$$k1_{15} = v15 + z25$$
$$k1_{16} = v16 + z26$$
$$k1_{17} = v17 + z27$$
$$k1_{18} = v18 + z28$$

$h11 + h21 + h13 + k1_{21} = v11 + z32 + z42$

$h11 + h12 + h22 + h14 + k1_{22} = v12 + z33 + z43$

$h11 + h12 + h13 + h23 + k1_{23} = v13 + z31 + z41 + z34 + z44$

$h12 + h14 + h24 + k1_{24} = v14 + z31 + z41$

$h01 + h02 + h03 + h04 + h31 + k1_{25} = v15 + z36 + z46 + z38 + z48$

$h02 + h03 + h04 + h32 + k1_{26} = v16 + z35 + z45 + z37 + z47$

$h03 + h04 + h33 + k1_{27} = v17 + z35 + z36 + z45 + z46 + z38 + z48$

$h01 + h02 + h03 + h34 + k1_{28} = v18 + z35 + z45 + z37 + z38 + z47 + z48$

$h01 + h03 + k1_{31} = v11 + z42 + z35 + z36 + z45 + z46$

$h01 + h02 + h04 + k1_{32} = v12 + z43 + z36 + z37 + z46 + z47$

$h01 + h02 + h03 + k1_{33} = v13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48$

$h02 + h04 + k1_{34} = v14 + z41 + z35 + z45 + z38 + z48$

$h11 + h12 + h13 + h14 + k1_{35} = v15 + z31 + z32 + z41 + z42 + z46 + z48$

$h12 + h13 + h14 + k1_{36} = v16 + z32 + z33 + z42 + z43 + z45 + z47$

$h13 + h14 + k1_{37} = v17 + z31 + z41 + z33 + z34 + z43 + z44 + z45 + z46 + z48$

$h11 + h12 + h13 + z31 + k1_{38} = v18 + z41 + z34 + z44 + z45 + z47 + z48$

$h01 + h03 + k1_{41} = v01 + z11 + z42 + z35 + z36 + z45 + z46$

$h01 + h02 + h04 + k1_{42} = v02 + z12 + z43 + z36 + z37 + z46 + z47$

$h01 + h02 + h03 + k1_{43} = v03 + z13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48$

$h02 + h04 + k1_{44} = v04 + z14 + z41 + z35 + z45 + z38 + z48$

$h11 + h12 + h13 + h14 + k1_{45} = v05 + z31 + z32 + z41 + z15 + z42 + z46 + z48$

$h12 + h13 + h14 + k1_{46} = v06 + z32 + z33 + z42 + z16 + z43 + z45 + z47$

$h13 + h14 + k1_{47} = v07 + z31 + z41 + z33 + z34 + z43 + z17 + z44 + z45 + z46 + z48$

$h11 + h12 + h13 + k1_{48} = v08 + z31 + z41 + z34 + z44 + z18 + z45 + z47 + z48$

$k2_{11} = v01 + v21 + z11$

$k2_{12} = v02 + v22 + z12$

$k2_{13} = v03 + v23 + z13$

$k2_{14} = v04 + v24 + z14$

$k2_{15} = v05 + v25 + z15$

$k2_{16} = v06 + v26 + z16$

$k2_{17} = v07 + v27 + z17$

$k2_{18} = v08 + v28 + z18$

$h02 + h12 + h21 + h31 + h23 + k2_{21} = v21 + z31 + z32 + z34 + z36 + z37 + z46 + z38 + z47 + z48$

$h03 + h21 + h13 + h22 + h32 + h24 + k2_{22} = v22 + z31 + z32 + z33 + z37 + z38 + z47 + z48$

$h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + k2_{23} = v23 + z31 + z32 + z33 + z34 + z38 + z48$

$h01 + h11 + h22 + h24 + h34 + k2_{24} = v24 + z31 + z33 + z35 + z36 + z45 + z37 + z46 + z38 + z47 + z48$

$h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + k2_{25} = v25 + z31 + z41 + z35 + z38$

$h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + k2_{26} = v26 + z32 + z42 + z35 + z36$

$h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + k2_{27} = v27 + z33 + z43 + z36 + z37$

$h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + k2_{28} = v28 + z34 + z44 + z37$

$h01 + h11 + h12 + h31 + h33 + k2_{31} = v21 + z32 + z41 + z33 + z34 + z43 + z35 + z36 + z37 + z46 + z38 + z47 + z48$

$h02 + h12 + h13 + h31 + h32 + h34 + k2_{32} = v22 + z41 + z33 + z42 + z34 + z44 + z36 + z37 + z38 + z47 + z48$

$h11 + h03 + h13 + h31 + h14 + h32 + h33 + k2_{33} = v23 + z41 + z42 + z34 + z43 + z37 + z38 + z48$

$h11 + h04 + h14 + h32 + h34 + k2_{34} = v24 + z31 + z32 + z33 + z42 + z34 + z35 + z44 + z36 + z45 + z37 + z46 + z47 + z48$

$h01 + h02 + h11 + h21 + h22 + h14 + h23 + h24 + k2_{35} = v25 + z31 + z32 + z41 + z33 + z34 + z35 + z48$

$h02 + h11 + h03 + h12 + h22 + h23 + h24 + k2_{36} = v26 + z32 + z33 + z42 + z34 + z36 + z45$

$h01 + h03 + h12 + h04 + h13 + h23 + h24 + k2_{37} = v27 + z33 + z34 + z43 + z37 + z46$

$h01 + h21 + h04 + h13 + h22 + h23 + z31 + z32 + k2_{38} = v28 + z33 + z44 + z38 + z47 + z48$

$h01 + h11 + h12 + h31 + h33 + k2_{41} = v11 + z21 + z32 + z41 + z33 + z34 + z43 + z35 + z36 + z37 + z46 + z38 + z47 + z48$

$h02 + h12 + h13 + h31 + h32 + h34 + k2_{42} = v12 + z22 + z41 + z33 + z42 + z34 + z44 + z36 + z37 + z38 + z47 + z48$

$h11 + h03 + h13 + h31 + h14 + h32 + h33 + k2_{43} = v13 + z23 + z41 + z42 + z34 + z43 + z37 + z38 + z48$

$h11 + h04 + h14 + h32 + h34 + k2_{44} = v14 + z31 + z32 + z24 + z33 + z42 + z34 + z35 + z44 + z36 + z45 + z37 + z46 + z47 + z48$

$h01 + h02 + h11 + h21 + h22 + h14 + h23 + h24 + k2_{45} = v15 + z31 + z32 + z41 + z33 + z25 + z34 + z35 + z48$

$h02 + h11 + h03 + h12 + h22 + h23 + h24 + k2_{46} = v16 + z32 + z33 + z42 + z34 + z26 + z36 + z45$

$h01 + h03 + h12 + h04 + h13 + h23 + h24 + k2_{47} = v17 + z33 + z34 + z43 + z27 + z37 + z46$

$h01 + h21 + h04 + h13 + h22 + h23 + z31 + k2_{48} = v18 + z32 + z33 + z44 + z28 + z38 + z47 + z48$

$k3_{11} = v11 + v31 + z21$

$k3_{12} = v12 + v32 + z22$

$k3_{13} = v13 + v33 + z23$

$k3_{14} = v14 + v34 + z24$

$k3_{15} = v15 + v35 + z25$

$k3_{16} = v16 + v36 + z26$

$k3_{17} = v17 + v37 + z27$

$k3_{18} = v18 + v38 + z28$

$h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + k3_{21} = v31 + z32 + z42 + z35 + z37$

$h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + k3_{22} = v32 + z33 + z43 + z35 + z36 + z38$

$h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + k3_{23} = v33 + z31 + z41 + z34 + z35 + z44 + z36 + z37$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + k3_{24} = v34 + z31 + z41 + z36 + z38$

$h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + k3_{25} = v35 + z31 + z33 + z35 + z36 + z45 + z37 + z46 + z47$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + z31 + k3_{26} = v36 + z32 + z34 + z35 + z36 + z45 + z37 + z46 + z38 + z47 + z48$

$h02 + h03 + h21 + h04 + h13 + h22 + h31 + h32 + h24 + h33 + h34 + z31 + z32 + k3_{27} = v37 + z33 + z36 + z37 + z46 + z38 + z47 + z48$

$h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + z32 + k3_{28} = v38 + z34 + z35 + z36 + z45 + z46 + z38 + z48$

$h01 + h02 + h03 + h21 + h04 + h22 + h31 + k3_{31} = v31 + z42 + z35 + z38 + z47 + z48$

$h02 + h03 + h04 + h22 + h23 + h32 + k3_{32} = v32 + z43 + z35 + z36 + z48$

$h03 + h21 + h04 + h23 + h24 + h33 + k3_{33} = v33 + z41 + z44 + z36 + z45 + z37$

$h01 + h02 + h03 + h21 + h24 + h34 + k3_{34} = v34 + z41 + z37 + z46 + z47 + z48$

$h11 + h12 + h21 + h13 + h24 + h33 + h34 + k3_{35} = v35 + z31 + z34 + z43 + z44 + z45 + z46 + z47$

$h11 + h12 + h21 + h13 + h22 + h14 + h34 + z31 + k3_{36} = v36 + z32 + z44 + z45 + z46 + z47 + z48$

$h12 + h13 + h22 + h31 + h14 + h23 + z32 + z41 + k3_{37} = v37 + z33 + z46 + z47 + z48$

$h11 + h12 + h14 + h23 + h32 + h33 + h34 + z33 + z42 + k3_{38} = v38 + z43 + z44 + z45 + z46 + z48$

$h01 + h02 + h03 + h21 + h04 + h22 + h31 + k3_{41} = v01 + v21 + z11 + z42 + z35 + z38 + z47 + z48$

$h02 + h03 + h04 + h22 + h23 + h32 + k3_{42} = v02 + v22 + z12 + z43 + z35 + z36 + z48$

$h03 + h21 + h04 + h23 + h24 + h33 + k3_{43} = v03 + v23 + z13 + z41 + z44 + z36 + z45 + z37$

$h01 + h02 + h03 + h21 + h24 + h34 + k3_{44} = v04 + v24 + z14 + z41 + z37 + z46 + z47 + z48$

$h11 + h12 + h21 + h13 + h24 + h33 + h34 + k3_{45} = v05 + v25 + z31 + z15 + z34 + z43 + z44 + z45 + z46 + z47$

$h11 + h12 + h21 + h13 + h22 + h14 + h34 + k3_{46} = v06 + v26 + z31 + z32 + z16 + z44 + z45 + z46 + z47 + z48$

$h12 + h13 + h22 + h31 + h14 + h23 + k3_{47} = v07 + v27 + z32 + z41 + z33 + z17 + z46 + z47 + z48$

$h11 + h12 + h14 + h23 + h32 + h33 + h34 + k3_{48} = v08 + v28 + z33 + z42 + z43 + z44 + z18 + z45 + z46 + z48$

$k4_{11} = v01 + v21 + v41 + z11$

$k4_{12} = v02 + v22 + v42 + z12$

$k4_{13} = v03 + v23 + v43 + z13$

$k4_{14} = v04 + v24 + v44 + z14$

$k4_{15} = v05 + v25 + v45 + z15$

$k4_{16} = v06 + v26 + v46 + z16$

$k4_{17} = v07 + v27 + v47 + z17$

$k4_{18} = v08 + v28 + v48 + z18$

$h01 + h11 + h03 + h12 + h13 + h23 + h33 + h34 + k4_{21} = v41 + z31 + z32 + z34 + z35 + z45 + z37 + z38 + z47 + z48$

$h01 + h02 + h11 + h12 + h21 + h04 + h13 + h14 + h24 + h34 + k4_{22} = v42 + z31 + z32 + z33 + z36 + z46 + z38 + z48$

$h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h14 + k4_{23} = v43 + z31 + z32 + z33 + z34 + z35 + z45 + z37 + z47$

$h02 + h11 + h12 + h04 + h22 + h14 + h32 + h33 + h34 + k4_{24} = v44 + z31 + z33 + z36 + z37 + z46 + z47$

$h01 + h11 + h03 + h12 + h21 + h04 + h31 + h33 + h34 + z31 + k4_{25} = v45 + z32 + z41 + z42 + z34 + z35 + z44 + z37 + z38$

$h02 + h12 + h04 + h13 + h22 + h32 + h34 + z31 + z32 + z41 + k4_{26} = v46 + z33 + z42 + z43 + z36 + z38$

$h01 + h11 + h03 + h13 + h31 + h14 + h23 + h33 + z31 + z32 + z41 + z33 + z42 + k4_{27} = v47 + z34 + z43 + z35 + z44 + z37$

$h02 + h11 + h03 + h14 + h32 + h24 + h33 + z31 + z41 + z33 + z43 + k4_{28} = v48 + z36 + z37$

$h02 + h04 + h13 + h14 + h33 + h34 + k4_{31} = v41 + z31 + z33 + z42 + z34 + z43 + z36 + z45 + z37 + z47 + z48$

$h01 + h03 + h14 + h34 + k4_{32} = v42 + z32 + z41 + z34 + z43 + z35 + z44 + z37 + z46 + z38 + z48$

$h01 + h02 + h11 + h04 + h31 + k4_{33} = v43 + z31 + z33 + z42 + z44 + z36 + z45 + z38 + z47$

$h01 + h03 + h12 + h04 + h13 + h14 + h32 + h33 + h34 + k4_{34} = v44 + z32 + z41 + z33 + z42 + z35 + z36 + z46 + z47$

$h01 + h02 + h11 + h03 + h21 + h04 + h22 + h31 + h23 + h34 + k4_{35} = v45 + z32 + z41 + z33 + z42 + z35 + z44 + z36 + z46 + z38 + z47$

$h02 + h03 + h12 + h21 + h04 + h22 + h31 + h23 + h32 + h24 + z31 + z41 + k4_{36} = v46 + z33 + z42 + z34 + z43 + z35 + z36 + z45 + z37 + z47 + z48$

$h03 + h04 + h13 + h22 + h23 + h32 + h24 + h33 + z32 + z41 + z42 + k4_{37} = v47 + z34 + z43 + z35 + z44 + z36 + z37 + z46 + z38 + z48$

$h01 + h02 + h03 + h21 + h22 + h14 + h24 + h33 + z31 + z32 + z41 + z43 + k4_{38} = v48 + z35 + z45 + z37 + z46$

$h02 + h04 + h13 + h14 + h33 + h34 + k4_{41} = v11 + v31 + z21 + z31 + z33 + z42 + z34 + z43 + z36 + z45 + z37 + z47 + z48$

$h01 + h03 + h14 + h34 + k4_{42} = v12 + v32 + z22 + z32 + z41 + z34 + z43 + z35 + z44 + z37 + z46 + z38 + z48$

$h01 + h02 + h11 + h04 + h31 + k4_{43} = v13 + v33 + z31 + z23 + z33 + z42 + z44 + z36 + z45 + z38 + z47$

$h01 + h03 + h12 + h04 + h13 + h14 + h32 + h33 + h34 + k4_{44} = v14 + v34 + z32 + z41 + z24 + z33 + z42 + z35 + z36 + z46 + z47$

$h01 + h02 + h11 + h03 + h21 + h04 + h22 + h31 + h23 + h34 + k4_{45} = v15 + v35 + z32 + z41 + z33 + z42 + z25 + z35 + z44 + z36 + z46 + z38 + z47$

$h02 + h03 + h12 + h21 + h04 + h22 + h31 + h23 + h32 + h24 + k4_{46} = v16 + z31 + v36 + z41 + z33 + z42 + z34 + z43 + z26 + z35 + z36 + z45 + z37 + z47 + z48$

$h03 + h04 + h13 + h22 + h23 + h32 + h24 + h33 + k4_{47} = v17 + z32 + z41 + v37 + z42 + z34 + z43 + z35 + z44 + z27 + z36 + z37 + z46 + z38 + z48$

$h01 + h02 + h03 + h21 + h22 + h14 + h24 + h33 + z31 + k4_{48} = v18 + z32 + z41 + v38 + z43 + z35 + z45 + z28 + z37 + z46$

$k5_{11} = v11 + v31 + v51 + z21$

$k5_{12} = v12 + v32 + v52 + z22$

$k5_{13} = v13 + v33 + v53 + z23$

$k5_{14} = v14 + v34 + v54 + z24$

$k5_{15} = v15 + v35 + v55 + z25$

$k5_{16} = v16 + v36 + v56 + z26$

$k5_{17} = v17 + v37 + v57 + z27$

$k5_{18} = v18 + v38 + v58 + z28$

$h02 + h21 + h13 + h22 + h23 + k5_{21} = v51 + z33 + z34 + z43 + z44 + z37$

$h11+h03+h21+h22+h14+h23+h24+k5_{22} = v52+z34+z35+z44+z38$

$h01+h11+h12+h04+h22+h23+h24+k5_{23} = v53+z31+z41+z35+z36$

$h01 + h12 + h21 + h22 + h24 + k5_{24} = v54 + z32 + z33 + z42 + z34 + z43 + z44 + z36$

$h02 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + k5_{25} = v55 + z33 + z36 + z46$

$h03+h04+h13+h22+h14+h23+h34+z31+k5_{26} = v56+z34+z37+z47$

$h21 + h04 + h31 + h14 + h23 + h24 + z31 + z32 + k5_{27} = v57 + z35 + z45 + z38 + z48$

$h01 + h02 + h11 + h03 + h12 + h21 + h04 + h13 + h14 + h32 + h24 + h33 + h34 + z32 + z35 + k5_{28} = v58 + z45$

$h02+h12+h04+h13+h23+h32+h24+h34+k5_{31} = v51+z43+z44+z47$

$h01+h11+h03+h13+h31+h14+h24+h33+k5_{32} = v52+z44+z45+z48$

$h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + k5_{33} = v53 + z41 + z45 + z46$

$h01+h11+h03+h12+h04+h22+h31+h23+h24+h33+h34+k5_{34} = v54 + z42 + z43 + z44 + z46$

$h11 + h21 + h14 + h34 + k5_{35} = v55 + z43 + z46$

$h11 + h12 + h22 + h31 + z41 + k5_{36} = v56 + z44 + z47$

$h12 + h13 + h23 + h32 + z41 + z42 + k5_{37} = v57 + z45 + z48$

$h13 + h24 + h33 + h34 + z42 + k5_{38} = v58 + z45$

$h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + k5_{41} = v01 + v21 + v41 + z11 + z43 + z44 + z47$

$h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + k5_{42} = v02 + v22 + v42 + z12 + z44 + z45 + z48$

$h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + k5_{43} = v03 + v23 + v43 + z13 + z41 + z45 + z46$

$h01+h11+h03+h12+h04+h22+h31+h23+h24+h33+h34+k5_{44} = v04 + v24 + v44 + z14 + z42 + z43 + z44 + z46$

$h11 + h21 + h14 + h34 + k5_{45} = v05 + v25 + v45 + z15 + z43 + z46$

$h11 + h12 + h22 + h31 + k5_{46} = v06 + v26 + z41 + v46 + z16 + z44 + z47$

$h12+h13+h23+h32+k5_{47} = v07+v27+z41+z42+v47+z17+z45+z48$

$h13 + h24 + h33 + h34 + k5_{48} = v08 + v28 + z42 + v48 + z18 + z45$

$\hbar 02+\hbar 21+\hbar 13+\hbar 22+\hbar 23+\bar{k}6_{11}=v11+v31+v51+v61+z21+z33+z34+z43+z44+z37$

$\hbar 11+\hbar 03+\hbar 21+\hbar 22+\hbar 14+\hbar 23+\hbar 24+\bar{k}6_{12}=v12+v32+v52+v62+z22+z34+z35+z44+z38$

$\hbar 01+\hbar 11+\hbar 12+\hbar 04+\hbar 22+\hbar 23+\hbar 24+\bar{k}6_{13}=v13+v33+v53+z31+v63+z23+z41+z35+z36$

$\hbar 01+\hbar 12+\hbar 21+\hbar 22+\hbar 24+\bar{k}6_{14}=v14+v34+v54+z32+v64+z24+z33+z42+z34+z43+z44+z36$

$\hbar 02+\hbar 03+\hbar 12+\hbar 21+\hbar 04+\hbar 13+\hbar 22+\hbar 14+\hbar 33+\hbar 34+\bar{k}6_{15}=v15+v35+v55+z33+v65+z25+z36+z46$

$\hbar 03+\hbar 04+\hbar 13+\hbar 22+\hbar 14+\hbar 23+\hbar 34+\bar{k}6_{16}=v16+z31+v36+v56+z34+v66+z26+z37+z47$

$\hbar 21+\hbar 04+\hbar 31+\hbar 14+\hbar 23+\hbar 24+\bar{k}6_{17}=v17+z31+z32+v37+v57+z35+v67+z27+z45+z38+z48$

$\hbar 01+\hbar 02+\hbar 11+\hbar 03+\hbar 12+\hbar 21+\hbar 04+\hbar 13+\hbar 14+\hbar 32+\hbar 24+\hbar 33+\hbar 34+\bar{k}6_{18}=v18+z32+v38+z35+v58+z45+v68+z28$

$\hbar 01+\hbar 02+\hbar 11+\hbar 03+\hbar 12+\hbar 04+\hbar 14+\hbar 23+\bar{k}6_{21}=v61+z32+z33+z42+z43+z35+z36+z38$

$\hbar 02+\hbar 11+\hbar 03+\hbar 12+\hbar 21+\hbar 04+\hbar 13+\hbar 24+\bar{k}6_{22}=v62+z31+z41+z33+z34+z43+z35+z44+z36+z37$

$\hbar 11+\hbar 03+\hbar 12+\hbar 21+\hbar 04+\hbar 13+\hbar 22+\hbar 14+\bar{k}6_{23}=v63+z32+z42+z34+z35+z44+z36+z37+z38$

$\hbar 01+\hbar 02+\hbar 11+\hbar 03+\hbar 13+\hbar 22+z31+z32+z41+\bar{k}6_{24}=v64+z42+z35+z37$

$\hbar 02+\hbar 12+\hbar 22+\hbar 23+\hbar 33+z31+z33+\bar{k}6_{25}=v65+z34+z36+z37+z46+z47$

$\hbar 03+\hbar 21+\hbar 13+\hbar 31+\hbar 23+\hbar 24+\hbar 34+z32+z34+\bar{k}6_{26}=v66+z35+z45+z37+z38+z47+z48$

$\hbar 01+\hbar 11+\hbar 04+\hbar 22+\hbar 31+\hbar 14+\hbar 32+\hbar 24+z31+z33+\bar{k}6_{27}=v67+z36+z46+z38+z48$

$\hbar 01+\hbar 11+\hbar 21+\hbar 22+\hbar 32+z32+z33+z35+z36+z45+\bar{k}6_{28}=v68+z46$

$\hbar 12+\hbar 04+\hbar 13+\hbar 22+\hbar 14+\hbar 23+\hbar 34+\bar{k}6_{31}=v61+z42+z43+z45+z46+z48$

$\hbar 01+\hbar 21+\hbar 13+\hbar 31+\hbar 14+\hbar 23+\hbar 24+\bar{k}6_{32}=v62+z41+z43+z44+z45+z46+z47$

$\hbar 02+\hbar 22+\hbar 14+\hbar 32+\hbar 24+\bar{k}6_{33}=v63+z42+z44+z45+z46+z47+z48$

$\hbar 11+\hbar 03+\hbar 12+\hbar 21+\hbar 04+\hbar 13+\hbar 22+\hbar 14+\hbar 33+\hbar 34+z41+\bar{k}6_{34}=v64+z42+z45+z47$

$\hbar 12+\hbar 21+\hbar 22+\hbar 31+\hbar 14+\hbar 34+z41+\bar{k}6_{35}=v65+z43+z44+z46+z47$

$h11+h13+h22+h31+h23+h32+z42+k6_{36}=v66+z44+z45+z47+z48$

$h11+h12+h21+h14+h23+h32+h24+h33+z41+z43+k6_{37}=v67+z46+z48$

$h11+h21+h13+h14+h24+h33+z42+z43+z45+k6_{38}=v68+z46$

$h12+h04+h13+h22+h14+h23+h34+k6_{41}=v01+v21+v41+z11+z42+z43+z45+z46+z48$

$h01+h21+h13+h31+h14+h23+h24+k6_{42}=v02+v22+v42+z12+z41+z43+z44+z45+z46+z47$

$h02+h22+h14+h32+h24+k6_{43}=v03+v23+v43+z13+z42+z44+z45+z46+z47+z48$

$h11+h03+h12+h21+h04+h13+h22+h14+h33+h34+k6_{44}=v04+v24+v44+z14+z41+z42+z45+z47$

$h12+h21+h22+h31+h14+h34+k6_{45}=v05+v25+v45+z41+z15+z43+z44+z46+z47$

$h11+h13+h22+h31+h23+h32+k6_{46}=v06+v26+v46+z42+z16+z44+z45+z47+z48$

$h11+h12+h21+h14+h23+h32+h24+h33+k6_{47}=v07+v27+z41+v47+z43+z17+z46+z48$

$h11+h21+h13+h14+h24+h33+k6_{48}=v08+v28+z42+z43+v48+z18+z45+z46$

$h01+h11+h03+h12+h13+h23+h33+h34+k7_{11}=v01+v21+v41+z11+v71+z31+z32+z34+z35+z45+z37+z38+z47+z48$

$h01+h02+h11+h12+h21+h04+h13+h14+h24+h34+k7_{12}=v02+v22+v42+z12+z31+v72+z32+z33+z36+z46+z38+z48$

$h01+h02+h03+h12+h21+h13+h22+h31+h14+k7_{13}=v03+v23+v43+z13+z31+z32+v73+z33+z34+z35+z45+z37+z47$

$h02+h11+h12+h04+h22+h14+h32+h33+h34+k7_{14}=v04+v24+v44+z31+z14+z33+v74+z36+z37+z46+z47$

$h01+h11+h03+h12+h21+h04+h31+h33+h34+k7_{15}=v05+v25+z31+v45+z32+z41+z15+z42+z34+v75+z35+z44+z37+z38$

$h02+h12+h04+h13+h22+h32+h34+k7_{16}=v06+v26+z31+z32+z41+v46+z33+z42+z16+z43+v76+z36+z38$

$h01+h11+h03+h13+h31+h14+h23+h33+k7_{17}=v07+z31+v27+z32+z41+z33+z42+v47+z34+z43+z17+z35+z44+v77+z37$

$h02+h11+h03+h14+h32+h24+h33+k7_{18}=v08+z31+z41+v28+z33+z43+v48+z18+z36+z37+v78$

$h01+h21+h13+h32+h33+k7_{21}=v71+z32+z37+z38+z47+z48$

$h02+h11+h22+h31+h14+h33+h34+k7_{22}=v72+z33+z38+z48$

$h11+h03+h12+h23+h32+h34+z31+k7_{23}=v73+z34+z35+z45$

$h12 + h04 + h31 + h32 + h24 + z31 + k7_{24} = v74 + z36 + z37 + z46 + z38 + z47 + z48$

$h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h32 + h33 + z33 + z34 + z43 + k7_{25} = v75 + z35 + z44 + z36 + z37$

$h01 + h02 + h11 + h03 + h04 + h13 + h22 + h31 + h14 + h23 + h32 + h33 + h34 + z34 + z35 + z44 + k7_{26} = v76 + z36 + z37 + z38$

$h02 + h03 + h12 + h21 + h04 + h14 + h23 + h32 + h24 + h33 + h34 + z31 + z41 + z36 + k7_{27} = v77 + z37 + z38$

$h01 + h02 + h11 + h12 + h21 + h04 + h31 + h32 + h24 + h34 + z32 + z33 + z42 + z34 + z43 + z35 + z44 + z36 + k7_{28} = v78 + z38$

$h12 + h04 + h13 + h32 + h33 + k7_{31} = v71 + z33 + z42 + z34 + z43 + z44 + z36 + z37 + z38 + z47 + z48$

$h01 + h11 + h13 + h31 + h14 + h33 + h34 + k7_{32} = v72 + z34 + z43 + z44 + z37 + z38 + z48$

$h02 + h12 + h14 + h32 + h34 + z31 + k7_{33} = v73 + z44 + z45 + z38$

$h11 + h03 + h12 + h04 + h31 + h32 + z32 + z41 + z33 + z42 + k7_{34} = v74 + z34 + z43 + z35 + z44 + z36 + z37 + z46 + z38 + z47 + z48$

$h01 + h11 + h12 + h32 + h24 + h34 + z31 + z32 + z34 + z43 + k7_{35} = v75 + z44 + z45 + z37 + z46 + z38 + z48$

$h02 + h12 + h21 + h13 + h31 + h33 + z31 + z32 + z33 + z44 + k7_{36} = v76 + z45 + z46 + z38 + z47$

$h11 + h03 + h13 + h22 + h31 + h14 + h32 + h34 + z31 + z32 + z41 + z33 + z34 + z35 + z45 + k7_{37} = v77 + z46 + z47 + z48$

$h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + z33 + z42 + z43 + z44 + z36 + z45 + z37 + k7_{38} = v78 + z38 + z47$

$h12 + h04 + h13 + h32 + h33 + k7_{41} = v11 + v31 + v51 + v61 + z21 + z33 + z42 + z34 + z43 + z44 + z36 + z37 + z38 + z47 + z48$

$h01 + h11 + h13 + h31 + h14 + h33 + h34 + k7_{42} = v12 + v32 + v52 + v62 + z22 + z34 + z43 + z44 + z37 + z38 + z48$

$h02 + h12 + h14 + h32 + h34 + k7_{43} = v13 + v33 + v53 + z31 + v63 + z23 + z44 + z45 + z38$

$h11 + h03 + h12 + h04 + h31 + h32 + k7_{44} = v14 + v34 + v54 + z32 + z41 + v64 + z24 + z33 + z42 + z34 + z43 + z35 + z44 + z36 + z37 + z46 + z38 + z47 + z48$

$h01 + h11 + h12 + h32 + h24 + h34 + k7_{45} = v15 + v35 + z31 + z32 + v55 + v65 + z25 + z34 + z43 + z44 + z45 + z37 + z46 + z38 + z48$

$h02 + h12 + h21 + h13 + h31 + h33 + k7_{46} = v16 + z31 + v36 + z32 + z33 + v56 + v66 + z26 + z44 + z45 + z46 + z38 + z47$

$h11 + h03 + h13 + h22 + h31 + h14 + h32 + h34 + k7_{47} = v17 + z31 + z32 + z41 + v37 + z33 + z34 + v57 + z35 + v67 + z27 + z45 + z46 + z47 + z48$

$h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + k7_{48} = v18 + z33 + z42 + v38 + z43 + z44 + v58 + z36 + z45 + v68 + z28 + z37 + z38 + z47$

$h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + k8_{11} = v11 + v31 + v51 + v61 + z21 + v81 + z32 + z42 + z35 + z37$

$h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + k8_{12} = v12 + v32 + v52 + v62 + z22 + v82 + z33 + z43 + z35 + z36 + z38$

$h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + k8_{13} = v13 + v33 + v53 + z31 + v63 + z23 + z41 + v83 + z34 + z35 + z44 + z36 + z37$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + k8_{14} = v14 + v34 + z31 + v54 + z41 + v64 + z24 + v84 + z36 + z38$

$h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + k8_{15} = v15 + v35 + z31 + v55 + z33 + v65 + z25 + z35 + v85 + z36 + z45 + z37 + z46 + z47$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + k8_{16} = v16 + z31 + v36 + z32 + v56 + z34 + v66 + z26 + z35 + z36 + z45 + v86 + z37 + z46 + z38 + z47 + z48$

$h02+h03+h21+h04+h13+h22+h31+h32+h24+h33+h34+k8_{17} = v17+z31+z32+v37+z33+v57+v67+z27+z36+z37+z46+v87+z38+z47+z48$

$h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + k8_{18} = v18 + z32 + v38 + z34 + z35 + v58 + z36 + z45 + v68 + z28 + z46 + z38 + v88 + z48$

$h01+h02+h11+h21+h23+h33+z31+k8_{21} = v81+z41+z33+z43+z35$

$h02+h03+h12+h21+h22+h31+h24+h34+z31+z32+z41+k8_{22} = v82 + z42 + z34 + z44 + z36$

$h01 + h03 + h21 + h04 + h13 + h22 + h31 + h23 + h32 + z31 + z32 + z41 + z33 + z42 + k8_{23} = v83 + z43 + z37$

$h01+h04+h22+h14+h32+h24+z32+z42+z34+k8_{24} = v84+z44+z38$

$h11 + h12 + h21 + h04 + h22 + h31 + h23 + h32 + h24 + h33 + h34 + z32 + z33 + z34 + k8_{25} = v85 + z38 + z48$

$h01 + h12 + h13 + h22 + h23 + h32 + h24 + h33 + h34 + z33 + z34 + z35 + z45 + k8_{26} = v86$

$h02+h11+h13+h14+h23+h24+h33+h34+z34+z36+z46+k8_{27} = v87$

$h11 + h03 + h21 + h04 + h22 + h31 + h14 + h23 + h32 + h33 + z31 + z32 + z33 + z34 + z37 + z38 + z47 + k8_{28} = v88 + z48$

$h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + k8_{31} = v81 + z41 + z43 + z35 + z36 + z37 + z46 + z47$

$h01 + h02 + h22 + h31 + h23 + h24 + h33 + z41 + k8_{32} = v82 + z42 + z35 + z44 + z36 + z45 + z37 + z38 + z47 + z48$

$h02 + h03 + h31 + h23 + h32 + h24 + h34 + z41 + z42 + k8_{33} = v83 + z43 + z36 + z37 + z46 + z38 + z48$

$h03 + h21 + h22 + h31 + h23 + h33 + h34 + z42 + k8_{34} = v84 + z35 +$

$z44 + z36 + z45 + z46 + z38$

$h22 + h14 + h24 + h33 + z32 + z34 + z43 + k8_{35} = v85 + z48$

$h11 + h21 + h31 + h23 + h34 + z31 + z41 + z33 + z44 + z45 + k8_{36} = v86$

$h12+h21+h22+h31+h32+h24+z31+z32+z41+z42+z34+z46+k8_{37} = v87$

$h21+h13+h14+h23+h32+h24+z31+z33+z42+z34+z47+k8_{38} = v88 + z48$

$h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + k8_{41} = v01 + v21 + v41 + z11 + v71 + z41 + z43 + z35 + z36 + z37 + z46 + z47$

$h01 + h02 + h22 + h31 + h23 + h24 + h33 + k8_{42} = v02 + v22 + v42 + z12 + v72 + z41 + z42 + z35 + z44 + z36 + z45 + z37 + z38 + z47 + z48$

$h02 + h03 + h31 + h23 + h32 + h24 + h34 + k8_{43} = v03 + v23 + v43 + z13 + z41 + v73 + z42 + z43 + z36 + z37 + z46 + z38 + z48$

$h03 + h21 + h22 + h31 + h23 + h33 + h34 + k8_{44} = v04 + v24 + v44 + z14 + z42 + v74 + z35 + z44 + z36 + z45 + z46 + z38$

$h22+h14+h24+h33+k8_{45} = v05+v25+v45+z32+z15+z34+z43+v75+z48$

$h11+h21+h31+h23+h34+k8_{46} = v06+v26+z31+z41+v46+z33+z16+z44+v76+z45$

$h12+h21+h22+h31+h32+h24+k8_{47} = v07+z31+v27+z32+z41+z42+v47+z34+z17+v77+z46$

$h21+h13+h14+h23+h32+h24+k8_{48} = v08+z31+v28+z33+z42+z34+v48+z18+v78+z47+z48$

$h02+h12+h21+h31+h23+k9_{11} = v01+v21+v41+z11+v71+z31+z32+v91+z34+z36+z37+z46+z38+z47+z48$

$h03+h21+h13+h22+h32+h24+k9_{12} = v02+v22+v42+z12+z31+v72+z32+z33+v92+z37+z38+z47+z48$

$h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + k9_{13} = v03 + v23 + v43 + z13 + z31 + z32 + v73 + z33 + z34 + v93 + z38 + z48$

$h01+h11+h22+h24+h34+k9_{14} = v04+v24+v44+z31+z14+z33+v74+z35+v94+z36+z45+z37+z46+z38+z47+z48$

$h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + k9_{15} = v05 + v25 + z31 + v45 + z41 + z15 + v75 + z35 + v95 + z38$

$h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + k9_{16} = v06 + v26 + z32 + v46 + z42 + z16 + z35 + v76 + z36 + v96$

$h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + k9_{17} = v07 + v27 + z33 + v47 + z43 + z17 + z36 + v77 + z37 + v97$

$h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + k9_{18} = v08 + v28 + z34 + v48 + z44 + z18 + z37 + v78 + v98$

$$h01 + h11 + h03 + h21 + h13 + z32 + k9_{21} = v91 + z35 + z36 + z45 + z46$$

$$h01 + h02 + h11 + h12 + h04 + h22 + h14 + z33 + k9_{22} = v92 + z36 + z37 + z46 + z47$$

$$h01 + h02 + h11 + h03 + h12 + h13 + h23 + z31 + z34 + k9_{23} = v03 + z35 + z45 + z37 + z38 + z47 + z48$$

$$h02 + h12 + h04 + h14 + h24 + z31 + z35 + k9_{24} = v94 + z45 + z38 + z48$$

$$h01 + h02 + h11 + h03 + h12 + h04 + h13 + h31 + h14 + z31 + z32 + z41 + z42 + z36 + k9_{25} = v05 + z38$$

$$h02 + h03 + h12 + h04 + h13 + h14 + h32 + z32 + z33 + z42 + z43 + z35 + z37 + k9_{26} = v96$$

$$h03 + h04 + h13 + h14 + h33 + z31 + z41 + z33 + z34 + z43 + z35 + z44 + z36 + z38 + k9_{27} = v97$$

$$h01 + h02 + h11 + h03 + h12 + h13 + h34 + z31 + z41 + z34 + z35 + z44 + z37 + z38 + k9_{28} = v98$$

Then, the next step S104 is executed to carry out a matricial-equation transformation process. In this process, vectors K, H, U and V are set as follows.

[formula 35]

$$K = (k1_{11}, K1_{12}, \ldots, k9_{28})$$
$$H = (h01, h02, \ldots, h44)$$
$$U = (z11, z12, \ldots, z44).$$
$$V = (v01, v02, \ldots v74)$$

With the vectors K, H, U and V set as expressed by the above equations, the simultaneous linear equation can be transformed into the following matricial equation.

[formula 36]

$$M_{KH}\begin{pmatrix} {}^{t}K \\ {}^{t}H \end{pmatrix} = M_{UV}\begin{pmatrix} {}^{t}U \\ {}^{t}V \end{pmatrix}$$

It is to be noted that, in the above equation, symbols M_{KH} and M_{UV} each denote a GF(2) matrix comprising coefficients of the simultaneous linear equation described above.

Then, the next step S105 is executed to carry out a unitary transformation process.

Let symbol N_r denote the rank value of the matrix M_{UV} as follows:

[formula 37]

$$\mathrm{rank}(M_{UV}) = N_r$$

Then, let symbol N_m denote the number of rows composing the matrix M_{UV}. By multiplying both the left-hand and right-hand sides of the matricial equation by a row-deform unitary matrix Q from the left, the matrix M_{UV} can be deformed into a step matrix. In this process, a small matrix consisting of $(N_m - N_r)$ lowest rows of the matrix QM_{UV} becomes a null matrix.

Then, the next step S106 is executed to carry out a small-matrix selection process. Let symbol M^*_{KH} denote a small matrix consisting of $(N_m - N_r)$ lowest rows of the matrix QM_{KH}. In this case, the small matrix M^*_{KH} becomes a null matrix (O) as expressed by the following equation.

[formula 38]

$$M^*_{KH} = O$$

Then, the next step S107 is executed to carry out a linear-relation equation generation process. This matricial equation is transformed into linear-relation equations, which are each associated with a row. Then, actual values are substituted for h01, h02, ··· and h44 to obtain the following relation equations:

[formula 39]

$$0x07 = k1_{11} + k1_{21} + k1_{24} + k1_{26} + k1_{31} + k1_{34} + k1_{36} + k1_{42} + k2_{12} + k2_{22} + k3_{11} + k3_{21}$$

$0x66 = k1_{12} + k1_{21} + k1_{22} + k1_{27} + k1_{31} + k1_{32} + k1_{37} + k1_{43} + k2_{13} + k2_{23} + k3_{12} + k3_{22}$

$0x9c = k1_{13} + k1_{22} + k1_{23} + k1_{25} + k1_{28} + k1_{32} + k1_{33} + k1_{35} + k1_{38} + k1_{41} + k1_{44} + k2_{11} + k2_{14} + k2_{21} + k2_{24} + k3_{13} + k3_{23}$

$0xdf = k1_{14} + k1_{23} + k1_{25} + k1_{33} + k1_{35} + k1_{41} + k2_{11} + k2_{21} + k3_{14} + k3_{24}$

$0xe9 = k1_{15} + k1_{22} + k1_{24} + k1_{25} + k1_{28} + k1_{32} + k1_{34} + k1_{35} + k1_{38} + k1_{46} + k1_{48} + k2_{16} + k2_{18} + k2_{26} + k2_{28} + k3_{15} + k3_{25}$

$0x23 = k1_{16} + k1_{21} + k1_{23} + k1_{26} + k1_{27} + k1_{31} + k1_{33} + k1_{36} + k1_{37} + k1_{45} + k1_{47} + k2_{15} + k2_{17} + k2_{25} + k2_{27} + k3_{16} + k3_{26}$

$0x60 = k1_{17} + k1_{21} + k1_{22} + k1_{24} + k1_{25} + k1_{27} + k1_{28} + k1_{31} + k1_{32} + k1_{34} + k1_{35} + k1_{37} + k1_{38} + k1_{45} + k1_{46} + k1_{48} + k2_{15} + k2_{16} + k2_{18} + k2_{25} + k2_{26} + k2_{28} + k3_{17} + k3_{27}$

$0xcd = k1_{18} + k1_{21} + k1_{23} + k1_{24} + k1_{25} + k1_{28} + k1_{31} + k1_{33} + k1_{34} + k1_{35} + k1_{38} + k1_{45} + k1_{47} + k1_{48} + k2_{15} + k2_{17} + k2_{18} + k2_{25} + k2_{27} + k2_{28} + k3_{18} + k3_{28}$

$0x3d = k1_{21} + k1_{24} + k1_{27} + k1_{28} + k1_{31} + k1_{34} + k1_{37} + k1_{38} + k1_{41} + k1_{42} + k1_{43} + k1_{48} + k2_{11} + k2_{12} + k2_{18} + k2_{21} + k2_{22} + k2_{23} + k2_{28} + k4_{13} + k4_{33}$

$0x90 = k1_{22} + k1_{25} + k1_{26} + k1_{27} + k1_{28} + k1_{32} + k1_{35} + k1_{36} + k1_{37} + k1_{38} + k1_{41} + k1_{43} + k1_{46} + k1_{47} + k1_{48} + k2_{13} + k2_{16} + k2_{17} + k2_{18} + k2_{21} + k2_{23} + k2_{26} + k2_{27} + k2_{28} + k4_{11} + k4_{31}$

$0xc1 = k1_{23} + k1_{26} + k1_{27} + k1_{28} + k1_{33} + k1_{36} + k1_{37} + k1_{38} + k1_{41} + k1_{42} + k1_{44} + k1_{47} + k1_{48} + k2_{11} + k2_{14} + k2_{17} + k2_{18} + k2_{21} + k2_{22} + k2_{24} + k2_{27} + k2_{28} + k4_{12} + k4_{32}$

$0x80 = k1_{24} + k1_{25} + k1_{26} + k1_{28} + k1_{34} + k1_{35} + k1_{36} + k1_{38} + k1_{41} + k1_{43} + k1_{44} + k1_{45} + k1_{46} + k1_{47} + k2_{11} + k2_{15} + k2_{16} + k2_{17} + k2_{21} + k2_{23} + k2_{24} + k2_{25} + k2_{26} + k2_{27} + k4_{13} + k4_{14} + k4_{33} + k4_{34}$

$0x39 = k1_{25} + k1_{35} + k1_{41} + k1_{44} + k1_{45} + k1_{47} + k1_{48} + k2_{11} + k2_{12} + k2_{14} + k2_{15} + k2_{16} + k2_{17} + k2_{18} + k2_{21} + k2_{24} + k2_{25} + k2_{27} + k2_{28} + k4_{12} + k4_{16} + k4_{32} + k4_{36}$

$0x2d = k1_{26} + k1_{36} + k1_{41} + k1_{42} + k1_{46} + k1_{48} + k2_{11} + k2_{12} + k2_{13} + k2_{16} + k2_{17} + k2_{18} + k2_{21} + k2_{22} + k2_{26} + k2_{28} + k4_{13} + k4_{17} + k4_{33} + k4_{37}$

$0xd5 = k1_{27} + k1_{28} + k1_{37} + k1_{38} + k1_{42} + k1_{45} + k1_{48} + k2_{12} + k2_{14} + k2_{15} + k2_{18} + k2_{18} + k2_{22} + k2_{25} + k2_{26} + k4_{14} + k4_{18} + k4_{34} + k4_{38}$

$0xfa = k1_{28} + k1_{38} + k1_{43} + k1_{46} + k1_{47} + k2_{11} + k2_{13} + k2_{15} + k2_{16} + k2_{17} + k2_{23} + k2_{26} + k2_{27} + k4_{11} + k4_{15} + k4_{31} + k4_{35}$

$0x39 = k1_{41} + k1_{42} + k1_{44} + k1_{46} + k1_{48} + k2_{12} + k2_{13} + k2_{17} + k2_{18} + k2_{22} + k2_{24} + k2_{26} + k2_{28} + k2_{31} + k4_{11} + k4_{13} + k4_{14} + k4_{16} + k4_{17} + k4_{31} + k4_{33} + k4_{34} + k4_{36} + k4_{37}$

$0x35 = k1_{42} + k1_{43} + k1_{44} + k1_{45} + k1_{46} + k1_{47} + k2_{11} + k2_{13} + k2_{16} + k2_{21} + k2_{22} + k2_{23} + k2_{25} + k2_{26} + k2_{27} + k2_{31} + k2_{33} + k4_{11} + k4_{12} + k4_{14} +$

$k4_{15} + k4_{17} + k4_{31} + k4_{32} + k4_{34} + k4_{35} + k4_{37}$

$0x4b = k1_{43}+k1_{44}+k1_{45}+k1_{46}+k1_{47}+k1_{48}+k2_{11}+k2_{12}+k2_{14}+k2_{17}+ k2_{21}+k2_{22}+k2_{23}+k2_{24}+k2_{25}+k2_{26}+k2_{27}+k2_{28}+k2_{31}+k2_{32}+k4_{11}+ k4_{12}+k4_{13}+k4_{15}+k4_{16}+k4_{18}+k4_{31}+k4_{32}+k4_{33}+k4_{35}+k4_{36}+k4_{38}$

$0xe7 = k1_{44}+k1_{46}+k1_{47}+k1_{48}+k2_{11}+k2_{12}+k2_{13}+k2_{16}+k2_{18}+ k2_{22}+k2_{23}+k2_{24}+k2_{26}+k2_{27}+k2_{28}+k2_{32}+k2_{33}+k4_{11}+k4_{12}+k4_{13}+ k4_{14}+k4_{15}+k4_{16}+k4_{17}+k4_{31}+k4_{32}+k4_{33}+k4_{34}+k4_{35}+k4_{36}+k4_{37}$

$0x33 = k1_{45}+k1_{48}+k2_{12}+k2_{13}+k3_{14}+k2_{16}+k2_{21}+k2_{25}+k2_{28}+k2_{31}+ k3_{11}+k4_{12}+k4_{13}+k4_{14}+k4_{16}+k4_{32}+k4_{33}+k4_{34}+k4_{35}+k5_{11}+k5_{21}$

$0xdb = k1_{46}+k1_{47}+k2_{13}+k2_{14}+k2_{17}+k2_{22}+k2_{26}+k2_{27}+k2_{32}+ k3_{12}+k4_{13}+k4_{14}+k4_{16}+k4_{33}+k4_{34}+k4_{36}+k5_{12}+k5_{22}$

$0x8f = k1_{47}+k1_{48}+k2_{11}+k2_{13}+k2_{14}+k2_{15}+k2_{16}+k2_{17}+k2_{21}+ k2_{22}+k2_{24}+k2_{27}+k2_{28}+k2_{31}+k2_{32}+k2_{34}+k3_{11}+k3_{12}+k3_{14}+k4_{11}+ k4_{13}+k4_{14}+k4_{15}+k4_{16}+k4_{18}+k4_{31}+k4_{33}+k4_{34}+k4_{35}+k4_{36}+k4_{38}+ k5_{11}+k5_{12}+k5_{14}+k5_{21}+k5_{22}+k5_{24}$

$0x83 = k1_{48}+k2_{12}+k2_{14}+k2_{15}+k2_{16}+k2_{17}+k2_{18}+k2_{21}+k2_{22}+k2_{23}+ k2_{28}+k2_{31}+k2_{32}+k2_{33}+k3_{11}+k3_{12}+k3_{13}+k4_{12}+k4_{14}+k4_{15}+k4_{16}+ k4_{17}+k4_{32}+k4_{34}+k4_{35}+k4_{36}+k4_{37}+k5_{11}+k5_{12}+k5_{13}+k5_{21}+k5_{22}+k5_{23}$

$0x00 = k2_{11} + k3_{11} + k4_{11} + k4_{31} + k4_{41}$

$0x00 = k2_{12} + k3_{12} + k4_{12} + k4_{32} + k4_{42}$

$0x00 = k2_{13} + k3_{13} + k4_{13} + k4_{33} + k4_{43}$

$0x00 = k2_{14} + k3_{14} + k4_{14} + k4_{34} + k4_{44}$

$0x1f = k2_{15}+k2_{17}+k2_{22}+k2_{23}+k2_{24}+k2_{25}+k2_{32}+k2_{33}+k2_{34}+k2_{35}+ k3_{11}+k3_{12}+k3_{13}+k3_{14}+k4_{15}+k4_{17}+k4_{35}+k4_{37}+k4_{41}+k4_{42}+k4_{43}+k4_{44}$

$0x8e = k2_{16}+k2_{17}+k2_{18}+k2_{22}+k2_{25}+k2_{26}+k2_{32}+k2_{35}+k2_{36}+ k3_{11}+k4_{16}+k4_{17}+k4_{18}+k4_{36}+k4_{37}+k4_{38}+k4_{41}$

$0x68 = k2_{17}+k2_{18}+k2_{23}+k2_{26}+k2_{27}+k2_{33}+k2_{36}+k2_{37}+k3_{12}+ k4_{17}+k4_{18}+k4_{37}+k4_{38}+k4_{42}$

$0x35 = k2_{18}+k2_{21}+k2_{24}+k2_{25}+k2_{27}+k2_{28}+k2_{31}+k2_{34}+k2_{35}+ k2_{37}+k2_{38}+k3_{13}+k4_{18}+k4_{38}+k4_{43}$

$0x42 = k2_{21}+k2_{22}+k2_{26}+k2_{28}+k2_{31}+k2_{32}+k2_{36}+k2_{38}+k3_{11}+ k3_{14}+k3_{15}+k4_{41}+k4_{44}+k4_{45}$

$0xe6 = k2_{22}+k2_{23}+k2_{25}+k2_{27}+k2_{32}+k2_{33}+k2_{35}+k2_{37}+k3_{11}+ k3_{12}+k3_{16}+k4_{41}+k4_{42}+k4_{46}$

$0x91 = k2_{23}+k2_{24}+k2_{26}+k2_{33}+k2_{34}+k2_{36}+k3_{12}+k3_{13}+k3_{14}+ k3_{15}+k3_{16}+k3_{18}+k4_{42}+k4_{43}+k4_{44}+k4_{45}+k4_{46}+k4_{48}$

$0xf9 = k2_{24}+k2_{27}+k2_{34}+k2_{37}+k3_{13}+k3_{14}+k3_{15}+k3_{16}+k3_{17}+ k4_{43}+k4_{44}+k4_{45}+k4_{46}+k4_{47}$

$0xa0 = k2_{25}+k2_{28}+k2_{35}+k2_{38}+k3_{11}+k3_{13}+k3_{15}+k4_{44}+k5_{11}+$

$k5_{13} + k5_{14} + k5_{15} + k5_{21} + k5_{23} + k5_{24} + k5_{25}$

$0xb7 = k2_{26} + k2_{28} + k2_{36} + k2_{38} + k3_{12} + k3_{13} + k3_{14} + k3_{15} + k3_{16} + k4_{41} + k4_{44} + k5_{11} + k5_{12} + k5_{13} + k5_{15} + k5_{16} + k5_{21} + k5_{22} + k5_{23} + k5_{25} + k5_{26}$

$0x07 = k2_{27} + k2_{28} + k2_{37} + k2_{38} + k3_{11} + k3_{14} + k3_{15} + k3_{16} + k3_{17} + k4_{41} + k4_{42} + k4_{44} + k5_{12} + k5_{15} + k5_{16} + k5_{17} + k5_{22} + k5_{25} + k5_{26} + k5_{27}$

$0xc1 = k2_{28} + k2_{38} + k3_{11} + k3_{12} + k3_{15} + k3_{16} + k3_{17} + k3_{18} + k4_{41} + k4_{42} + k4_{43} + k5_{13} + k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{23} + k5_{25} + k5_{26} + k5_{27} + k5_{28}$

$0xc9 = k2_{41} + k3_{11} + k3_{12} + k3_{13} + k3_{16} + k3_{17} + k3_{21} + k4_{41} + k4_{42} + k4_{43} + k4_{47} + k4_{48} + k5_{11} + k5_{16} + k5_{18} + k5_{21} + k5_{26} + k5_{28}$

$0xed = k2_{42} + k3_{11} + k3_{12} + k3_{13} + k3_{14} + k3_{15} + k3_{17} + k3_{18} + k3_{22} + k4_{41} + k4_{42} + k4_{43} + k4_{44} + k4_{48} + k5_{12} + k5_{15} + k5_{17} + k5_{22} + k5_{25} + k5_{27}$

$0xf6 = k2_{43} + k3_{12} + k3_{13} + k3_{14} + k3_{16} + k3_{18} + k3_{23} + k4_{42} + k4_{43} + k4_{44} + k4_{45} + k5_{13} + k5_{15} + k5_{16} + k5_{18} + k5_{23} + k5_{25} + k5_{26} + k5_{28}$

$0x46 = k2_{44} + k3_{11} + k3_{12} + k3_{14} + k3_{15} + k3_{16} + k3_{24} + k4_{41} + k4_{42} + k4_{44} + k4_{46} + k4_{47} + k4_{48} + k5_{14} + k5_{15} + k5_{17} + k5_{18} + k5_{24} + k5_{25} + k5_{27} + k5_{28}$

$0x81 = k2_{45} + k3_{11} + k3_{14} + k3_{15} + k3_{16} + k3_{17} + k3_{18} + k3_{25} + k4_{41} + k4_{43} + k4_{46} + k4_{48} + k5_{13} + k5_{14} + k5_{17} + k5_{23} + k5_{24} + k5_{27}$

$0x29 = k2_{46} + k3_{11} + k3_{12} + k3_{16} + k3_{17} + k3_{18} + k3_{26} + k4_{41} + k4_{42} + k4_{44} + k4_{45} + k4_{47} + k5_{14} + k5_{16} + k5_{18} + k5_{24} + k5_{25} + k5_{28}$

$0x85 = k2_{47} + k3_{12} + k3_{13} + k3_{17} + k3_{18} + k3_{27} + k4_{41} + k4_{42} + k4_{43} + k4_{45} + k4_{46} + k4_{48} + k5_{11} + k5_{15} + k5_{16} + k5_{21} + k5_{25} + k5_{26}$

$0x69 = k2_{48} + k3_{13} + k3_{15} + k3_{16} + k3_{17} + k3_{28} + k4_{42} + k4_{44} + k4_{45} + k4_{47} + k4_{48} + k5_{12} + k5_{13} + k5_{14} + k5_{16} + k5_{22} + k5_{23} + k5_{24} + k5_{28}$

$0x7b = k3_{11} + k3_{12} + k3_{16} + k3_{17} + k3_{18} + k4_{11} + k4_{41} + k4_{43} + k5_{16} + k5_{17} + k5_{18} + k5_{26} + k5_{27} + k5_{28} + k5_{41}$

$0x1b = k3_{12} + k3_{13} + k3_{14} + k3_{16} + k4_{11} + k4_{12} + k4_{42} + k4_{43} + k4_{44} + k5_{15} + k5_{26} + k5_{41} + k5_{42}$

$0xbc = k3_{13} + k3_{14} + k3_{17} + k4_{12} + k4_{13} + k4_{43} + k4_{44} + k5_{17} + k5_{27} + k5_{42} + k5_{43}$

$0x53 = k3_{14} + k3_{15} + k3_{18} + k4_{11} + k4_{13} + k4_{14} + k4_{44} + k5_{15} + k5_{18} + k5_{25} + k5_{28} + k5_{41} + k5_{43} + k5_{44}$

$0x04 = k3_{15} + k3_{17} + k4_{11} + k4_{12} + k4_{13} + k4_{15} + k4_{41} + k4_{44} + k4_{45} + k4_{46} + k4_{47} + k4_{48} + k5_{11} + k5_{14} + k5_{16} + k5_{18} + k5_{21} + k5_{24} + k5_{26} + k5_{28} + k5_{41} + k5_{42} + k5_{43} + k5_{45}$

$0xcf = k3_{16} + k3_{17} + k3_{18} + k4_{14} + k4_{15} + k4_{16} + k4_{42} + k4_{44} + k4_{45} + k5_{12} + k5_{14} + k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{22} + k5_{24} + k5_{25} + k5_{26} + k5_{27} + k5_{28} + k5_{44} + k5_{45} + k5_{46}$

$0x58 = k3_{17} + k3_{18} + k4_{11} + k4_{16} + k4_{17} + k4_{41} + k4_{43} + k4_{46} + k5_{11} + k5_{13} + k5_{16} + k5_{17} + k5_{18} + k5_{21} + k5_{23} + k5_{26} + k5_{27} + k5_{28} + k5_{41} + k5_{46} + k5_{47}$

$0x21 = k3_{18} + k4_{12} + k4_{15} + k4_{17} + k4_{18} + k4_{41} + k4_{42} + k4_{44} + k4_{47} + k5_{11} + k5_{12} + k5_{14} + k5_{17} + k5_{18} + k5_{21} + k5_{22} + k5_{24} + k5_{27} + k5_{28} + k5_{42} + k5_{45} + k5_{47} + k5_{48}$

$0x37 = k3_{21} + k3_{31} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{44} + k4_{45} + k4_{47} + k5_{11} + k5_{14} + k5_{15} + k5_{17} + k5_{21} + k5_{24} + k5_{25} + k5_{27} + k5_{41} + k5_{42} + k5_{43} + k5_{44} + k5_{46} + k5_{47} + k5_{48}$

$0xa3 = k3_{22} + k3_{32} + k4_{12} + k4_{13} + k4_{14} + k4_{17} + k4_{18} + k4_{41} + k4_{42} + k4_{45} + k4_{46} + k4_{48} + k5_{11} + k5_{12} + k5_{15} + k5_{16} + k5_{18} + k5_{21} + k5_{22} + k5_{25} + k5_{26} + k5_{28} + k5_{42} + k5_{43} + k5_{44} + k5_{47} + k5_{48}$

$0x9b = k3_{23} + k3_{33} + k4_{13} + k4_{14} + k4_{18} + k4_{42} + k4_{43} + k4_{45} + k4_{46} + k4_{47} + k5_{12} + k5_{13} + k5_{15} + k5_{16} + k5_{17} + k5_{22} + k5_{23} + k5_{25} + k5_{26} + k5_{27} + k5_{43} + k5_{44} + k5_{48}$

$0x51 = k3_{24} + k3_{34} + k4_{11} + k4_{12} + k4_{13} + k4_{15} + k4_{16} + k4_{17} + k4_{18} + k4_{43} + k4_{46} + k4_{48} + k5_{13} + k5_{16} + k5_{18} + k5_{23} + k5_{26} + k5_{28} + k5_{41} + k5_{42} + k5_{43} + k5_{45} + k5_{46} + k5_{47} + k5_{48}$

$0x4a = k3_{25} + k3_{35} + k4_{12} + k4_{14} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{46} + k4_{47} + k5_{11} + k5_{16} + k5_{17} + k5_{21} + k5_{26} + k5_{27} + k5_{42} + k5_{44} + k5_{46} + k5_{47} + k5_{48}$

$0x5f = k3_{26} + k3_{36} + k4_{11} + k4_{13} + k4_{17} + k4_{18} + k4_{42} + k4_{45} + k4_{47} + k4_{48} + k5_{12} + k5_{15} + k5_{17} + k5_{18} + k5_{22} + k5_{25} + k5_{27} + k5_{28} + k5_{41} + k5_{43} + k5_{47} + k5_{48}$

$0x9a = k3_{27} + k3_{37} + k4_{11} + k4_{12} + k4_{14} + k4_{18} + k4_{43} + k4_{46} + k4_{48} + k5_{13} + k5_{15} + k5_{18} + k5_{23} + k5_{25} + k5_{28} + k5_{41} + k5_{42} + k5_{44} + k5_{48}$

$0xc2 = k3_{28} + k3_{38} + k4_{11} + k4_{13} + k4_{14} + k4_{15} + k4_{16} + k4_{17} + k4_{18} + k4_{44} + k4_{45} + k4_{48} + k5_{14} + k5_{15} + k5_{18} + k5_{24} + k5_{25} + k5_{28} + k5_{41} + k5_{42} + k5_{44} + k5_{45} + k5_{46} + k5_{47} + k5_{48}$

$0x72 = k3_{41} + k4_{14} + k4_{16} + k4_{31} + k4_{43} + k4_{47} + k5_{13} + k5_{17} + k5_{23} + k5_{27} + k5_{41} + k5_{44} + k5_{48}$

$0xa2 = k3_{42} + k4_{11} + k4_{15} + k4_{32} + k4_{41} + k4_{44} + k4_{45} + k4_{48} + k5_{11} + k5_{14} + k5_{15} + k5_{18} + k5_{21} + k5_{24} + k5_{25} + k5_{28} + k5_{41} + k5_{42} + k5_{45}$

$0x68 = k3_{43} + k4_{12} + k4_{16} + k4_{33} + k4_{41} + k4_{42} + k4_{45} + k4_{46} + k5_{11} + k5_{12} + k5_{15} + k5_{16} + k5_{21} + k5_{22} + k5_{25} + k5_{26} + k5_{42} + k5_{43} + k5_{46}$

$0x56 = k3_{44} + k4_{13} + k4_{14} + k4_{17} + k4_{18} + k4_{34} + k4_{42} + k4_{46} + k5_{12} + k5_{16} + k5_{22} + k5_{26} + k5_{43} + k5_{47} + k5_{48}$

$0x80 = k3_{45} + k4_{12} + k4_{13} + k4_{16} + k4_{18} + k4_{35} + k4_{42} + k4_{43} + k4_{47} + k5_{12} + k5_{13} + k5_{17} + k5_{22} + k5_{23} + k5_{27} + k5_{42} + k5_{43} + k5_{45} + k5_{46} + k5_{48}$

$0xda = k3_{46} + k4_{11} + k4_{13} + k4_{14} + k4_{15} + k4_{17} + k4_{36} + k4_{41} + k4_{43} + k4_{44} + k4_{45} + k4_{48} + k5_{11} + k5_{13} + k5_{14} + k5_{15} + k5_{18} + k5_{21} + k5_{23} + k5_{24} + k5_{25} + k5_{28} + k5_{41} + k5_{43} + k5_{44} + k5_{45} + k5_{46} + k5_{47}$

$0xc7 = k3_{47} + k4_{12} + k4_{14} + k4_{15} + k4_{16} + k4_{18} + k4_{37} + k4_{42} + k4_{44} + k4_{45} + k4_{46} + k5_{12} + k5_{14} + k5_{15} + k5_{16} + k5_{22} + k5_{24} + k5_{25} + k5_{26} + k5_{42} +$

$k5_{44} + k5_{45} + k5_{46} + k5_{47} + k5_{48}$

$0x2c = k3_{48} + k4_{11} + k4_{12} + k4_{15} + k4_{17} + k4_{18} + k4_{38} + k4_{41} + k4_{42} + k4_{46} + k5_{11} + k5_{12} + k5_{16} + k5_{21} + k5_{22} + k5_{26} + k5_{41} + k5_{42} + k5_{45} + k5_{47}$

$0x5e = k4_{11} + k4_{13} + k4_{14} + k4_{15} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{44} + k4_{46} + k4_{48} + k5_{14} + k5_{16} + k5_{18} + k5_{21} + k5_{24} + k5_{26} + k5_{28} + k5_{41} + k5_{43} + k5_{44} + k5_{45} + k5_{46} + k5_{47} + k5_{48} + k6_{11} + k6_{31}$

$0x69 = k4_{12} + k4_{14} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{42} + k4_{45} + k4_{47} + k5_{11} + k5_{15} + k5_{17} + k5_{21} + k5_{22} + k5_{25} + k5_{27} + k5_{42} + k5_{44} + k5_{46} + k5_{47} + k5_{48} + k6_{12} + k6_{32}$

$0x66 = k4_{13} + k4_{14} + k4_{15} + k4_{18} + k4_{41} + k4_{42} + k4_{43} + k4_{48} + k5_{11} + k5_{13} + k5_{14} + k5_{18} + k5_{21} + k5_{22} + k5_{23} + k5_{28} + k5_{43} + k5_{44} + k5_{45} + k5_{48} + k6_{12} + k6_{14} + k6_{32} + k6_{34}$

$0x94 = k4_{14} + k4_{15} + k4_{16} + k4_{41} + k4_{42} + k4_{43} + k4_{44} + k4_{45} + k5_{12} + k5_{14} + k5_{15} + k5_{21} + k5_{22} + k5_{23} + k5_{24} + k5_{25} + k5_{44} + k5_{45} + k5_{46} + k6_{11} + k6_{13} + k6_{31} + k6_{33}$

$0x8f = k4_{15} + k4_{16} + k4_{41} + k4_{42} + k4_{43} + k4_{44} + k5_{15} + k5_{21} + k5_{22} + k5_{23} + k5_{24} + k5_{43} + k5_{46} + k6_{11} + k6_{12} + k6_{13} + k6_{14} + k6_{15} + k6_{31} + k6_{32} + k6_{33} + k6_{34} + k6_{35}$

$0x1b = k4_{16} + k4_{17} + k4_{42} + k4_{43} + k4_{44} + k5_{16} + k5_{22} + k5_{23} + k5_{24} + k5_{46} + k5_{47} + k6_{12} + k6_{13} + k6_{14} + k6_{16} + k6_{32} + k6_{33} + k6_{34} + k6_{36}$

$0x48 = k4_{17} + k4_{18} + k4_{42} + k4_{43} + k5_{15} + k5_{16} + k5_{18} + k5_{22} + k5_{23} + k5_{47} + k5_{48} + k6_{12} + k6_{13} + k6_{15} + k6_{16} + k6_{18} + k6_{32} + k6_{33} + k6_{35} + k6_{36} + k6_{38}$

$0x28 = k4_{18} + k4_{41} + k4_{43} + k4_{44} + k5_{15} + k5_{16} + k5_{17} + k5_{21} + k5_{23} + k5_{24} + k5_{48} + k6_{11} + k6_{13} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{31} + k6_{33} + k6_{34} + k6_{35} + k6_{36} + k6_{37}$

$0x00 = k4_{21} + k4_{31} + k4_{45} + k5_{25} + k6_{15} + k6_{35}$

$0x00 = k4_{22} + k4_{32} + k4_{46} + k5_{26} + k6_{16} + k6_{36}$

$0x00 = k4_{23} + k4_{33} + k4_{47} + k5_{27} + k6_{17} + k6_{37}$

$0x00 = k4_{24} + k4_{34} + k4_{48} + k5_{28} + k6_{18} + k6_{38}$

$0x00 = k4_{25} + k4_{35} + k4_{41} + k5_{21} + k6_{11} + k6_{31}$

$0x00 = k4_{26} + k4_{36} + k4_{42} + k5_{22} + k6_{12} + k6_{32}$

$0x00 = k4_{27} + k4_{37} + k4_{43} + k5_{23} + k6_{13} + k6_{33}$

$0x00 = k4_{28} + k4_{38} + k4_{44} + k5_{24} + k6_{14} + k6_{34}$

$0x7b = k4_{41} + k4_{43} + k5_{16} + k5_{17} + k5_{18} + k5_{21} + k5_{23} + k5_{45} + k6_{11} + k6_{13} + k6_{16} + k6_{17} + k6_{18} + k6_{31} + k6_{33} + k6_{36} + k6_{37} + k6_{38} + k6_{45}$

$0x1b = k4_{42} + k4_{43} + k4_{44} + k5_{16} + k5_{22} + k5_{23} + k5_{24} + k5_{45} + k5_{46} + k6_{12} + k6_{13} + k6_{14} + k6_{16} + k6_{32} + k6_{33} + k6_{34} + k6_{36} + k6_{45} + k6_{46}$

$0xbc = k4_{43} + k4_{44} + k5_{17} + k5_{23} + k5_{24} + k5_{46} + k5_{47} + k6_{13} + k6_{14} + k6_{17} + k6_{33} + k6_{34} + k6_{37} + k6_{46} + k6_{47}$

$0x53 = k4_{44} + k5_{25} + k5_{18} + k5_{24} + k5_{45} + k5_{47} + k5_{48} + k6_{14} + k6_{15} + k6_{18} + k6_{34} + k6_{35} + k6_{38} + k6_{45} + k6_{47} + k6_{48}$

$0x79 = k4_{45} + k4_{46} + k4_{47} + k5_{13} + k5_{25} + k5_{26} + k5_{27} + k5_{41} + k6_{13} + k6_{15} + k6_{16} + k6_{17} + k6_{33} + k6_{32} + k6_{35} + k6_{37} + k6_{41}$

$0xd8 = k4_{46} + k4_{47} + k4_{48} + k5_{11} + k5_{12} + k5_{26} + k5_{27} + k5_{28} + k5_{43} + k6_{11} + k6_{12} + k6_{16} + k6_{17} + k6_{18} + k6_{31} + k6_{32} + k6_{36} + k6_{37} + k6_{38} + k6_{43}$

$0xfb = k4_{47} + k4_{48} + k5_{12} + k5_{13} + k5_{27} + k5_{28} + k5_{41} + k5_{44} + k6_{12} + k6_{13} + k6_{17} + k6_{18} + k6_{32} + k6_{33} + k6_{37} + k6_{38} + k6_{41} + k6_{44}$

$0xba = k4_{48} + k5_{11} + k5_{13} + k5_{14} + k5_{28} + k5_{41} + k5_{42} + k6_{11} + k6_{13} + k6_{14} + k6_{18} + k6_{31} + k6_{33} + k6_{34} + k6_{38} + k6_{41} + k6_{42}$

$0x04 = k5_{11} + k5_{14} + k5_{15} + k5_{44} + k5_{45} + k5_{48} + k6_{11} + k6_{14} + k6_{15} + k6_{31} + k6_{34} + k6_{35} + k6_{43} + k6_{44} + k6_{45} + k6_{48} + k7_{13} + k7_{23}$

$0x25 = k5_{12} + k5_{17} + k5_{18} + k5_{42} + k5_{43} + k5_{44} + k5_{46} + k6_{12} + k6_{17} + k6_{18} + k6_{32} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{46} + k7_{11} + k7_{21}$

$0x96 = k5_{13} + k5_{18} + k5_{43} + k5_{44} + k5_{47} + k6_{13} + k6_{18} + k6_{33} + k6_{38} + k6_{42} + k6_{43} + k6_{44} + k6_{47} + k7_{12} + k7_{22}$

$0xca = k5_{14} + k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{42} + k5_{43} + k5_{48} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{34} + k6_{35} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k6_{48} + k7_{13} + k7_{14} + k7_{23} + k7_{24}$

$0x94 = k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{44} + k5_{48} + k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{35} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{43} + k6_{48} + k7_{12} + k7_{14} + k7_{21} + k7_{23} + k7_{24} + k7_{31}$

$0xa7 = k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{42} + k5_{45} + k6_{16} + k6_{17} + k6_{18} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k6_{45} + k7_{14} + k7_{22} + k7_{24} + k7_{32}$

$0xef = k5_{17} + k5_{18} + k5_{42} + k5_{43} + k5_{48} + k6_{17} + k6_{18} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{45} + k7_{11} + k7_{21} + k7_{22} + k7_{33}$

$0xe7 = k5_{18} + k5_{41} + k5_{43} + k5_{44} + k5_{47} + k6_{18} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{47} + k7_{12} + k7_{21} + k7_{22} + k7_{24} + k7_{31} + k7_{34}$

$0x69 = k5_{21} + k5_{31} + k5_{41} + k5_{43} + k5_{44} + k6_{41} + k6_{43} + k6_{44} + k7_{22} + k7_{32}$

$0xca = k5_{22} + k5_{32} + k5_{42} + k5_{44} + k6_{42} + k6_{44} + k7_{23} + k7_{33}$

$0x51 = k5_{23} + k5_{33} + k5_{41} + k5_{43} + k6_{41} + k6_{43} + k7_{21} + k7_{24} + k7_{31} + k7_{34}$

$0x5e = k5_{24} + k5_{34} + k5_{42} + k5_{43} + k6_{42} + k6_{43} + k7_{21} + k7_{31}$

$0x33 = k5_{25} + k5_{35} + k5_{42} + k5_{44} + k5_{48} + k6_{42} + k6_{43} + k6_{44} + k6_{48} + k7_{13} + k7_{21} + k7_{22} + k7_{23} + k7_{31} + k7_{32}$

$0x48 = k5_{26} + k5_{36} + k5_{41} + k5_{43} + k5_{45} + k6_{43} + k6_{44} + k6_{45} + k7_{11} + k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33}$

$0x28 = k5_{27} + k5_{37} + k5_{41} + k5_{42} + k5_{44} + k5_{46} + k6_{44} + k6_{46} + k7_{11} + k7_{12} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34}$

$0xc7 = k5_{28} + k5_{38} + k5_{41} + k5_{43} + k5_{44} + k5_{47} + k5_{48} + k6_{41} + k6_{42} +$

$k6_{33} + k6_{44} + k6_{47} + k6_{48} + k7_{12} + k7_{21} + k7_{22} + k7_{24} + k7_{31} + k7_{34}$

$0x09 = k5_{41} + k5_{42} + k5_{43} + k5_{44} + k6_{11} + k6_{41} + k6_{43} + k7_{13} + k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{32} + k7_{41}$

$0x16 = k5_{42} + k5_{43} + k5_{44} + k6_{12} + k6_{42} + k6_{43} + k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{42}$

$0xde = k5_{43} + k5_{44} + k6_{13} + k6_{41} + k6_{43} + k6_{44} + k7_{11} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34} + k7_{43}$

$0x2c = k5_{44} + k6_{11} + k6_{14} + k6_{42} + k6_{44} + k7_{12} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k7_{44}$

$0x02 = k5_{46} + k5_{47} + k6_{12} + k6_{13} + k6_{14} + k6_{16} + k6_{42} + k6_{43} + k6_{44} + k6_{45} + k6_{47} + k7_{12} + k7_{13} + k7_{14} + k7_{22} + k7_{23} + k7_{34} + k7_{42} + k7_{43} + k7_{44} + k7_{46}$

$0x43 = k5_{46} + k5_{48} + k6_{11} + k6_{12} + k6_{13} + k6_{14} + k6_{15} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{45} + k6_{48} + k7_{11} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{23} + k7_{33} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{45}$

$0x7d = k5_{47} + k6_{11} + k6_{13} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{41} + k6_{43} + k6_{44} + k6_{47} + k7_{11} + k7_{13} + k7_{14} + k7_{24} + k7_{31} + k7_{33} + k7_{41} + k7_{43} + k7_{44} + k7_{45} + k7_{46} + k7_{47}$

$0x57 = k5_{48} + k6_{11} + k6_{14} + k6_{16} + k6_{18} + k6_{41} + k6_{44} + k6_{48} + k7_{11} + k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{41} + k7_{44} + k7_{45} + k7_{48}$

$0x37 = k6_{11} + k6_{14} + k6_{22} + k6_{32} + k6_{42} + k7_{12} + k7_{21} + k7_{22} + k7_{31} + k7_{41} + k7_{44}$

$0x94 = k6_{12} + k6_{14} + k6_{22} + k6_{23} + k6_{32} + k6_{33} + k6_{42} + k6_{43} + k7_{12} + k7_{13} + k7_{21} + k7_{23} + k7_{31} + k7_{32} + k7_{42} + k7_{44}$

$0x51 = k6_{13} + k6_{21} + k6_{31} + k6_{41} + k7_{11} + k7_{21} + k7_{24} + k7_{34} + k7_{43}$

$0x5e = k6_{14} + k6_{22} + k6_{23} + k6_{24} + k6_{32} + k6_{33} + k6_{34} + k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{31} + k7_{32} + k7_{33} + k7_{34} + k7_{44}$

$0x33 = k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{22} + k6_{24} + k6_{26} + k6_{32} + k6_{34} + k6_{35} + k6_{41} + k7_{11} + k7_{21} + k7_{45} + k7_{46} + k7_{47} + k7_{48}$

$0x48 = k6_{16} + k6_{17} + k6_{18} + k6_{21} + k6_{23} + k6_{26} + k6_{31} + k6_{33} + k6_{36} + k6_{42} + k7_{12} + k7_{22} + k7_{46} + k7_{47} + k7_{48}$

$0x28 = k6_{17} + k6_{18} + k6_{21} + k6_{22} + k6_{24} + k6_{27} + k6_{31} + k6_{32} + k6_{34} + k6_{37} + k6_{43} + k7_{13} + k7_{23} + k7_{47} + k7_{48}$

$0xf4 = k6_{18} + k6_{21} + k6_{22} + k6_{23} + k6_{25} + k6_{28} + k6_{31} + k6_{32} + k6_{33} + k6_{35} + k6_{38} + k6_{41} + k6_{44} + k7_{11} + k7_{14} + k7_{21} + k7_{24} + k7_{48}$

$0xf7 = k6_{21} + k6_{25} + k6_{31} + k6_{35} + k6_{41} + k7_{11} + k7_{22} + k7_{24} + k7_{31} + k7_{32} + k7_{34} + k7_{43} + k8_{13} + k8_{23}$

$0xcc = k6_{22} + k6_{23} + k6_{24} + k6_{26} + k6_{27} + k6_{28} + k6_{32} + k6_{33} + k6_{34} + k6_{36} + k6_{37} + k6_{38} + k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{22} + k7_{31} + k7_{33} + k7_{34} + k7_{44} + k8_{14} + k8_{24}$

$0x52 = k6_{23} + k6_{24} + k6_{27} + k6_{28} + k6_{33} + k6_{34} + k6_{37} + k6_{38} + k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{22} + k7_{23} + k7_{32} + k7_{34} + k7_{41} + k8_{11} + k8_{21}$

$0xf8 = k6_{24} + k6_{25} + k6_{34} + k6_{33} + k6_{44} + k7_{14} + k7_{21} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{42} + k8_{12} + k8_{22}$

$0xf9 = k6_{25} + k6_{27} + k6_{28} + k6_{35} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k7_{11} + k7_{12} + k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{46} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{16} + k8_{21} + k8_{22} + k8_{23} + k8_{24} + k8_{25}$

$0x60 = k6_{26} + k6_{27} + k6_{36} + k6_{37} + k6_{41} + k6_{43} + k7_{11} + k7_{13} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{45} + k8_{11} + k8_{12} + k8_{13} + k8_{15} + k8_{21} + k8_{22} + k8_{23} + k8_{25}$

$0xc1 = k6_{27} + k6_{28} + k6_{37} + k6_{38} + k6_{42} + k7_{12} + k7_{21} + k7_{22} + k7_{31} + k7_{41} + k7_{44} + k7_{45} + k7_{47} + k8_{11} + k8_{14} + k8_{15} + k8_{17} + k8_{22} + k8_{24} + k8_{25} + k8_{27}$

$0xc0 = k6_{34} + k6_{38} + k6_{43} + k7_{13} + k7_{22} + k7_{23} + k7_{32} + k7_{41} + k7_{42} + k7_{45} + k7_{46} + k7_{48} + k8_{11} + k8_{12} + k8_{15} + k8_{16} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{26} + k8_{28}$

$0x2c = k6_{41} + k6_{43} + k7_{11} + k7_{13} + k7_{21} + k7_{22} + k7_{24} + k7_{32} + k7_{33} + k7_{34} + k7_{41} + k7_{43} + k7_{44} + k7_{45} + k8_{11} + k8_{13} + k8_{14} + k8_{15} + k8_{23} + k8_{24} + k8_{25} + k8_{31}$

$0xf5 = k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{23} + k7_{24} + k7_{32} + k7_{41} + k7_{42} + k7_{43} + k7_{45} + k7_{46} + k8_{11} + k8_{12} + k8_{13} + k8_{15} + k8_{16} + k8_{23} + k8_{25} + k8_{26} + k8_{31} + k8_{32}$

$0x08 = k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{24} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{46} + k7_{47} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{16} + k8_{17} + k8_{21} + k8_{24} + k8_{26} + k8_{27} + k8_{32} + k8_{33}$

$0xc9 = k6_{44} + k7_{14} + k7_{21} + k7_{31} + k7_{34} + k7_{42} + k7_{43} + k7_{44} + k7_{45} + k7_{47} + k7_{48} + k8_{12} + k8_{13} + k8_{14} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{26} + k8_{27} + k8_{28} + k8_{31} + k8_{33} + k8_{34}$

$0xcd = k6_{45} + k7_{15} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{25} + k7_{31} + k7_{32} + k7_{33} + k7_{34} + k7_{41} + k7_{46} + k7_{48} + k8_{11} + k8_{16} + k8_{18} + k8_{22} + k8_{23} + k8_{26} + k8_{28} + k8_{31} + k8_{32} + k8_{33}$

$0xfd = k6_{46} + k7_{16} + k7_{22} + k7_{23} + k7_{24} + k7_{26} + k7_{32} + k7_{53} + k7_{34} + k7_{42} + k7_{45} + k7_{47} + k8_{12} + k8_{16} + k8_{17} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{27} + k8_{31} + k8_{32} + k8_{33} + k8_{34}$

$0xe1 = k6_{47} + k7_{17} + k7_{23} + k7_{24} + k7_{27} + k7_{33} + k7_{34} + k7_{43} + k7_{45} + k7_{46} + k7_{48} + k8_{12} + k8_{15} + k8_{16} + k8_{18} + k8_{22} + k8_{24} + k8_{25} + k8_{26} + k8_{28} + k8_{32} + k8_{33} + k8_{34}$

$0xc9 = k6_{48} + k7_{13} + k7_{21} + k7_{22} + k7_{23} + k7_{28} + k7_{31} + k7_{32} + k7_{33} + k7_{44} + k7_{45} + k7_{47} + k7_{48} + k8_{14} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{27} + k8_{28} + k8_{31} + k8_{32} + k8_{34}$

$0x0a = k7_{11} + k7_{23} + k7_{24} + k7_{33} + k7_{34} + k7_{43} + k7_{44} + k8_{13} + k8_{14} + k8_{22} + k8_{32} + k8_{33} + k8_{34} + k8_{41}$

$0x0d = k7_{12} + k7_{24} + k7_{34} + k7_{44} + k8_{14} + k8_{23} + k8_{33} + k8_{34} + k8_{42}$

$0xc0 = k7_{13} + k7_{21} + k7_{31} + k7_{41} + k8_{11} + k8_{21} + k8_{24} + k8_{34} + k8_{43}$

$0xa4 = k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{34} + k7_{42} + k7_{43} +$
$k7_{44} + k8_{12} + k8_{13} + k8_{14} + k8_{21} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{44}$

$0x8c = k7_{15} + k7_{21} + k7_{22} + k7_{31} + k7_{32} + k7_{42} + k7_{43} + k7_{44} + k7_{45} +$
$k8_{12} + k8_{13} + k8_{14} + k8_{15} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{31} + k8_{32} + k8_{45}$

$0xdb = k7_{16} + k7_{22} + k7_{23} + k7_{32} + k7_{33} + k7_{43} + k7_{44} + k7_{46} + k8_{13} +$
$k8_{14} + k8_{16} + k8_{23} + k8_{24} + k8_{26} + k8_{32} + k8_{33} + k8_{46}$

$0x58 = k7_{17} + k7_{21} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34} + k7_{44} + k7_{47} +$
$k8_{14} + k8_{17} + k8_{21} + k8_{23} + k8_{27} + k8_{31} + k8_{33} + k8_{34} + k8_{47}$

$0x2e = k7_{18} + k7_{21} + k7_{24} + k7_{31} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{48} +$
$k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{18} + k8_{22} + k8_{23} + k8_{28} + k8_{31} + k8_{34} + k8_{48}$

$0x91 = k7_{21} + k7_{24} + k7_{31} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k8_{11} +$
$k8_{12} + k8_{13} + k8_{14} + k8_{23} + k8_{24} + k8_{26} + k8_{31} + k8_{32} + k8_{35}$

$0x68 = k7_{22} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k8_{11} + k8_{23} + k8_{26} + k8_{27} +$
$k8_{31} + k8_{33} + k8_{36} + k8_{37}$

$0x1f = k7_{23} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k8_{11} + k8_{12} + k8_{13} + k8_{22} +$
$k8_{23} + k8_{24} + k8_{25} + k8_{31} + k8_{34} + k8_{35}$

$0xbb = k7_{24} + k7_{34} + k7_{42} + k7_{44} + k8_{12} + k8_{14} + k8_{21} + k8_{22} + k8_{24} +$
$k8_{26} + k8_{27} + k8_{28} + k8_{31} + k8_{36} + k8_{37} + k8_{38}$

$0xe6 = k7_{25} + k7_{35} + k7_{45} + k7_{46} + k7_{47} + k7_{48} + k8_{15} + k8_{16} + k8_{17} +$
$k8_{18} + k8_{22} + k8_{23} + k8_{25} + k8_{27} + k8_{32} + k8_{33} + k8_{36} + k8_{38}$

$0x5d = k7_{26} + k7_{36} + k7_{46} + k7_{47} + k7_{48} + k8_{16} + k8_{17} + k8_{18} + k8_{21} +$
$k8_{23} + k8_{24} + k8_{25} + k8_{26} + k8_{28} + k8_{31} + k8_{33} + k8_{34} + k8_{35} + k8_{37}$

$0x77 = k7_{27} + k7_{37} + k7_{47} + k7_{48} + k8_{17} + k8_{18} + k8_{22} + k8_{24} + k8_{25} +$
$k8_{26} + k8_{27} + k8_{32} + k8_{34} + k8_{35} + k8_{36} + k8_{38}$

$0x42 = k7_{28} + k7_{38} + k7_{45} + k7_{46} + k7_{47} + k8_{15} + k8_{16} + k8_{17} + k8_{21} +$
$k8_{22} + k8_{26} + k8_{28} + k8_{31} + k8_{32} + k8_{35} + k8_{37} + k8_{38}$

$0x78 = k7_{41} + k7_{45} + k7_{46} + k7_{48} + k8_{11} + k8_{15} + k8_{16} + k8_{18} + k8_{22} +$
$k8_{24} + k8_{26} + k8_{31} + k8_{32} + k8_{34} + k8_{35} + k8_{38} + k8_{41} + k9_{11} + k9_{21}$

$0x85 = k7_{42} + k7_{45} + k7_{46} + k7_{47} + k8_{12} + k8_{15} + k8_{16} + k8_{17} + k8_{21} +$
$k8_{23} + k8_{27} + k8_{31} + k8_{32} + k8_{33} + k8_{35} + k8_{36} + k8_{42} + k9_{12} + k9_{22}$

$0x16 = k7_{43} + k7_{45} + k7_{46} + k7_{47} + k7_{48} + k8_{13} + k8_{15} + k8_{16} + k8_{17} +$
$k8_{18} + k8_{21} + k8_{22} + k8_{24} + k8_{25} + k8_{28} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{36} +$
$k8_{37} + k8_{43} + k9_{13} + k9_{23}$

$0x24 = k7_{44} + k7_{45} + k7_{47} + k8_{14} + k8_{16} + k8_{17} + k8_{21} + k8_{23} + k8_{24} +$
$k8_{26} + k8_{31} + k8_{33} + k8_{37} + k8_{44} + k9_{14} + k9_{24}$

$0x7c = k7_{45} + k7_{47} + k7_{48} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{26} +$
$k8_{27} + k8_{28} + k8_{31} + k8_{32} + k8_{36} + k8_{43} + k8_{46} + k9_{13} + k9_{16} + k9_{23} + k9_{26}$

$$0x42 = k7_{46} + k7_{47} + k8_{16} + k8_{17} + k8_{21} + k8_{24} + k8_{25} + k8_{26} + k8_{27} + k8_{31} + k8_{34} + k8_{35} + k8_{42} + k8_{45} + k9_{12} + k9_{15} + k9_{22} + k9_{25}$$

$$0x5d = k7_{47} + k7_{48} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{23} + k8_{24} + k8_{25} + k8_{28} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{35} + k8_{37} + k8_{41} + k8_{42} + k8_{44} + k8_{45} + k8_{47} + k9_{11} + k9_{12} + k9_{14} + k9_{15} + k9_{17} + k9_{21} + k9_{22} + k9_{24} + k9_{25} + k9_{27}$$

$$0x56 = k7_{48} + k8_{18} + k8_{22} + k8_{23} + k8_{24} + k8_{25} + k8_{26} + k8_{32} + k8_{33} + k8_{34} + k8_{35} + k8_{36} + k8_{38} + k8_{41} + k8_{42} + k8_{43} + k8_{45} + k8_{46} + k8_{48} + k9_{11} + k9_{12} + k9_{13} + k9_{15} + k9_{16} + k9_{18} + k9_{21} + k9_{22} + k9_{23} + k9_{25} + k9_{26} + k9_{28}$$

Here, the following equation holds true.

[formula 40]

$$\mathrm{rank}(M^*_{KH}) = N_m - N_r$$

Thus, the above 168 linear-relation equations are linear-relation equations independent of each other. It is therefore obvious that $(2^{168} - 1)$ linear-relation equations obtained from linear concatenation of any of the 168 equations on the GF(2) hold true. If the number of such linear-relation equations is large, it is feared that a new attack that the designer of the encryption method is not aware of is brought about. For this reason, the total number of linear-relation equations obtained by adoption of the method described above can be used as an indicator for the evaluation of the encryption level.

The present invention has been described in detail by referring to the specific embodiments. It is obvious, however, that a person skilled in the art is capable of correcting and modifying the embodiments within a range not deviating from the principle of the present invention.

That is to say, the embodiments are explained only for the purpose of disclosing the present invention and not to be interpreted as limitations imposed on the present invention. The scope of the present invention should thus be determined by referring to claims appended at the end of this specification.

It is to be noted that the series of processes explained in this specification can be carried out by using hardware, software or a combination of hardware and software. In the case of software used as an execution means, a program prescribing the series of processes is executed. The program is installed in advance in a memory employed in a computer including embedded special hardware or a general-purpose computer capable or carrying out various kinds of processing. Typically, the program is recorded in advance in a recording medium embedded in the computer. Examples of the embedded recording medium are a hard disc or a ROM (Read Only Memory).

As an alternative, the program is stored (or recorded) in advance in a removable recording medium temporarily of permanently. Examples of the removable recording medium are a flexible disc, a CD-ROM (Compact Disc Read Only Memory), an MO (Magneto-optical) disc, a

DVD (Digital Versatile Disc), a magnetic disc and a semiconductor memory. Then, the program recorded on the removable recording medium is presented to the user as the so-called package software. The program is then installed in the computer from the removable recording medium described above.

It is to be noted, however, that the program can also be downloaded to the computer from a download site by a wireless communication or by a wire communication through a network instead of being presented to the user by using a removable recording medium. Examples of the network are a LAN (Local Area Network) and the Internet. The computer includes functions to receive the downloaded program and install the received program in the embedded recording medium such as a hard disc.

It is to be noted that the various kinds of processing described in this specification can be carried out not only sequentially in accordance with a predetermined sequence but also concurrently or individually in accordance with the processing capacity of the apparatus for performing the processing or in accordance with the necessity.

As described above, in accordance with the configuration of the present invention, it is possible to comprehend all equations expressing linear relations among round keys in the common-key block encryption method without regard to the complexity of key scheduling and possible to evaluate the encryption level of the common-key block encryption method on the basis of the derived equations expressing linear relations among round keys.

In addition, in accordance with the configuration of the present invention, the key-scheduling part algorithm, which is one of encryption algorithms, is expressed in terms of equations represented by vectors and a matrix and, then, non-linear transformation output values and initial values are eliminated from the matricial equation by carrying out a unitary transformation process in order to find all equations expressing linear relations among round keys. If the relations among the round keys are simple dependence relations, the number of true round keys decreases. Thus, the designer of the encryption method needs to use caution so as to prevent a large number of such relation equations from existing. In accordance with the method provided by the present invention, the level of encryption keys is evaluated for the purpose of reducing the number of equations expressing linear relations among round keys. As a result, a safer encryption method can be designed.